CSC 515 : Software Security

Report 1

INDEX

Security test planning and execution

Test Case 1:

Test case	ASVS	Unique ID	CWE
1	5.3.4	5.3.4-1	89

ASVS 5.3.4: Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks

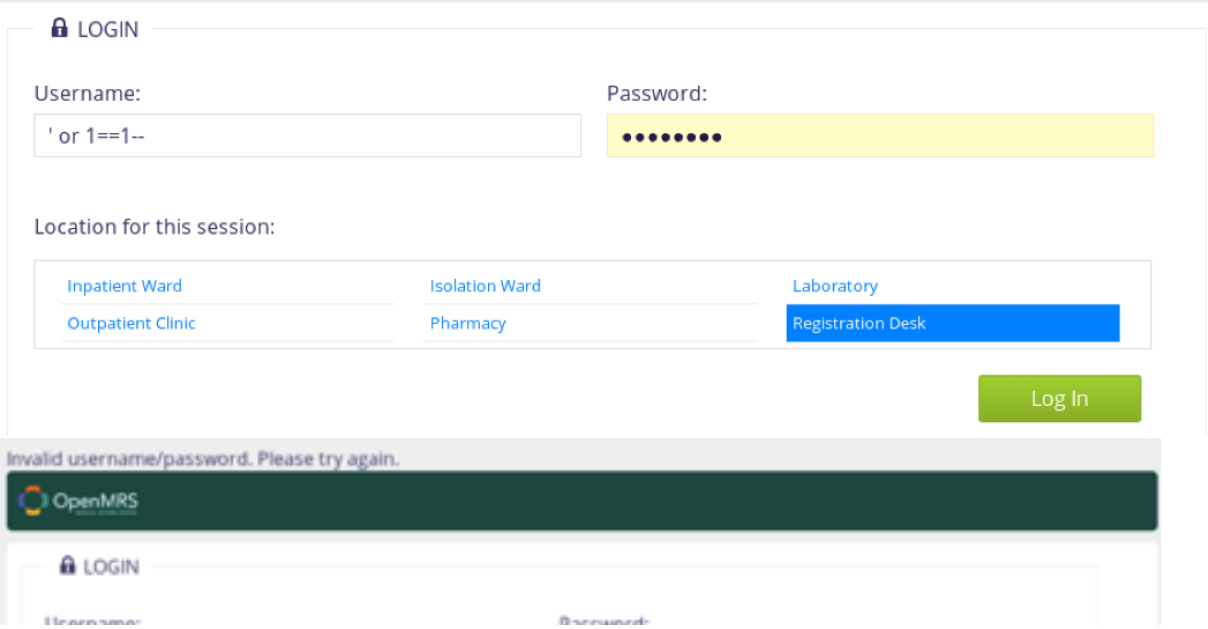
CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
The software constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Repeatable Steps:
1. Go to the login page - http://localhost:8080/openmrs/login.htm
2. Enter "‘ or 1==1--"as the username and password as "abc123"
3. Click login.

Actual Result:
The login page displays error message.

Expected Result:
An error should be displayed, since it is not a valid username.

Result: Passed



Test Case 2:

Test Case	ASVS	Unique ID	CWE
2	2.1.1	2.1.1-1	521

ASVS 2.1.1:
Verify that user set passwords are at least 12 characters in length.

CWE-521: Weak Password Requirements
The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

Repeatable steps:

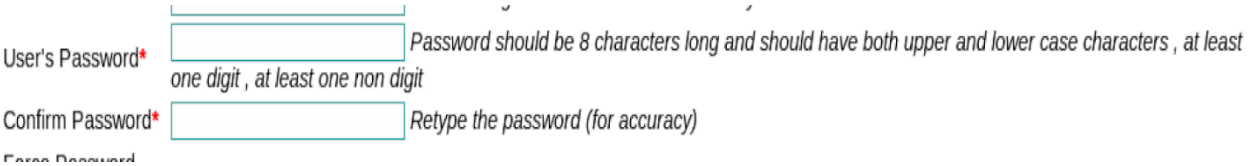
1. Login as admin by entering the username as “admin” and password as “Admin123”.
2. Click on System Administration
3. Click on advanced administration

4. Click on manage users
5. Click on Add user
6. Under ‘create a new person’ click on next

Actual Result:
Minimum password length is set to 8 characters.

Expected result:
As described in ASVS 2.1.1, minimum password length should be 12 characters.

Result: Failed



Test Case 3

Test Case	ASVS	Unique ID	CWE
3	2.1.6	2.1.6-1	620

ASVS 2.1.6:
Verify users can change their password.

CWE-620: Unverified Password Change
When setting a new password for a user, the product does not require knowledge of the original password or using another form of authentication.

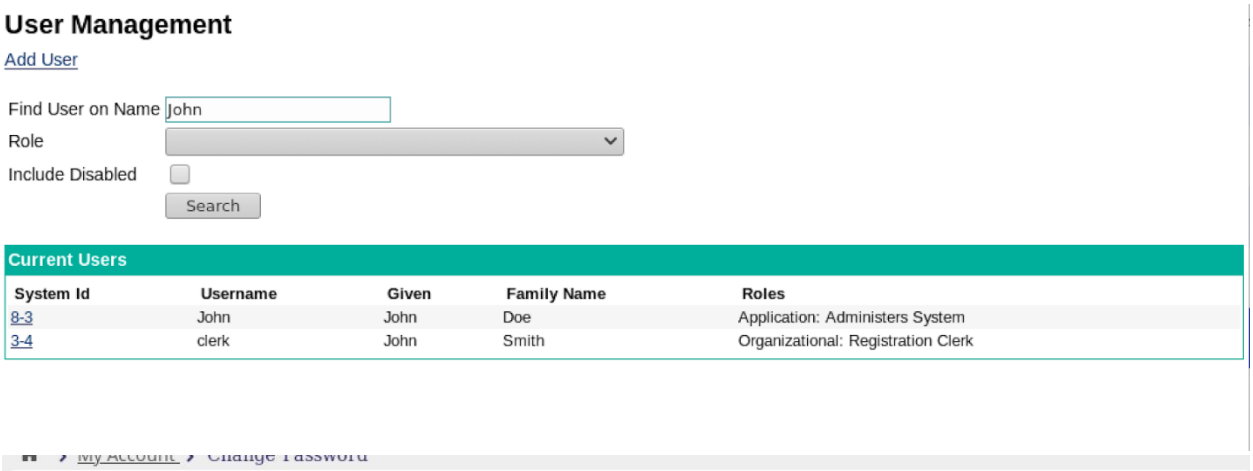
Repeatable steps:
1. Login as admin by entering username as “admin” and password as “Admin123”.
2. Click on System Administration
3. Click on Advanced administration
4. Click on Manage users

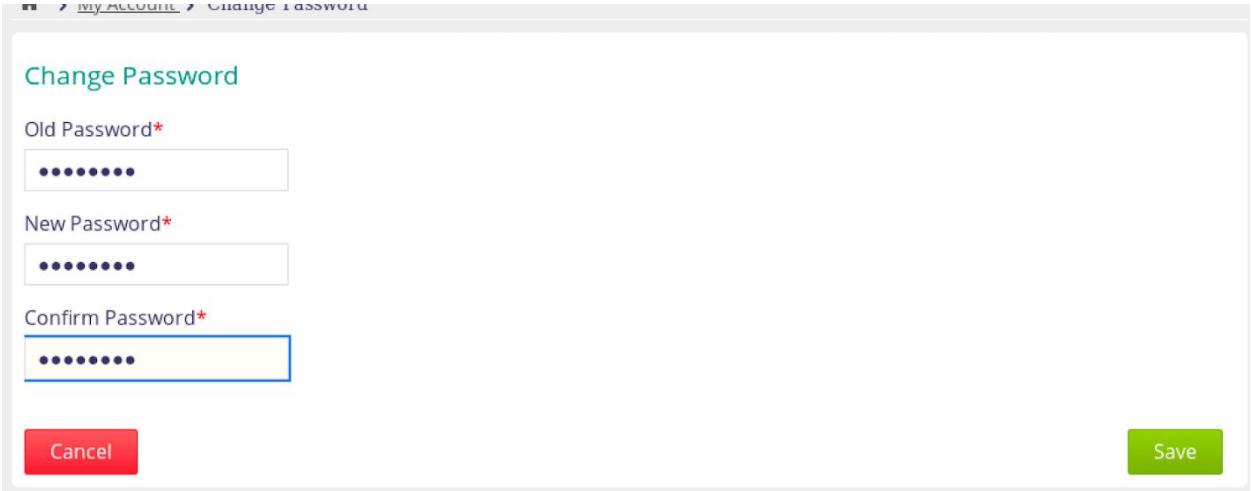
5. Click on Add user
6. Under ‘create a new person’ click on next.
7. Enter details.
8. Check Force password change
9. Logout.
10. Login again with details given in step 7.

Actual Result:
It requests for old and new password.

Expected Result:
Users should be able to update old password.

Result:
Passed





Test case 4:

Test Case	ASVS	Unique ID	CWE
4	1.4.4	1.4.4-1	284

ASVS 1.4.4:
Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.

CWE: Improper Access Control
The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

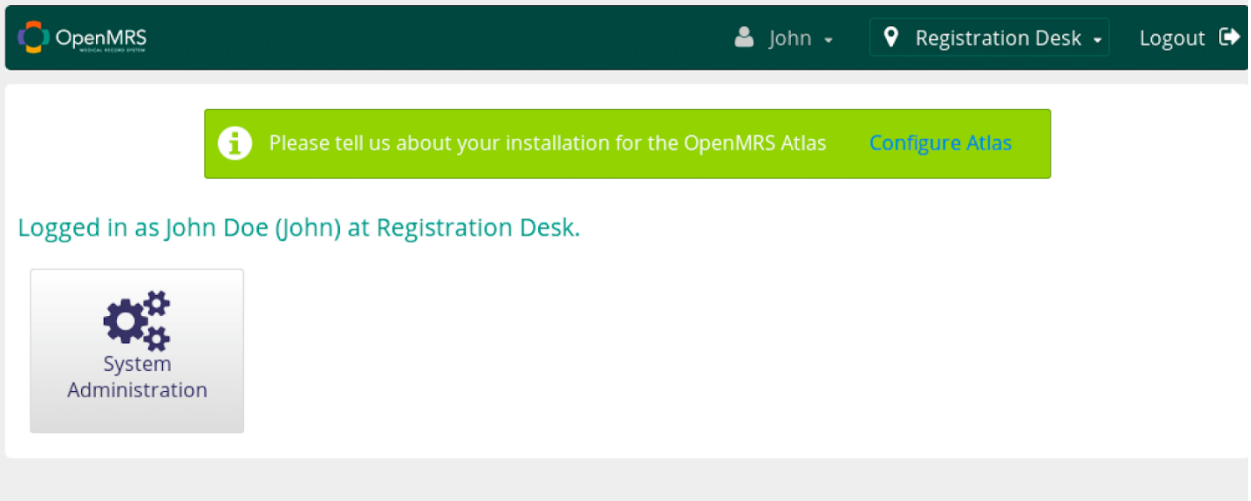
Repeatable steps:

1. Login as admin by entering username as “admin” and password as “Admin123”.
2. Click on active visits.
3. Copy the URL from the address bar - http://localhost:8080/openmrs/coreapps/activeVisits.page?app=coreapps.activeVisits
4. Logout.
5. Login as user ‘John Doe’, Password - Abcd1234 (This user has only system admin rights)
6. Paste the link from step 3 in the address bar - http://localhost:8080/openmrs/coreapps/activeVisits.page?app=coreapps.activeVisits

Actual Result:
User ‘John Doe’ is able to access this page

Expected Result:
Application should display an error stating that the user does not have rights

Result: Failed



Test Case 5:

Test Case	ASVS	Unique ID	CWE
5	7.4.2	7.4.2-1	544

ASVS 7.4.2:
Verify that exception handling (or a functional equivalent) is used across the codebase to account for expected and unexpected error conditions.

CWE Missing Standardized Error Handling Mechanism:
The software does not use a standardized method for handling errors throughout the code, which might introduce inconsistent error handling and resultant weaknesses.

Repeatable Steps:

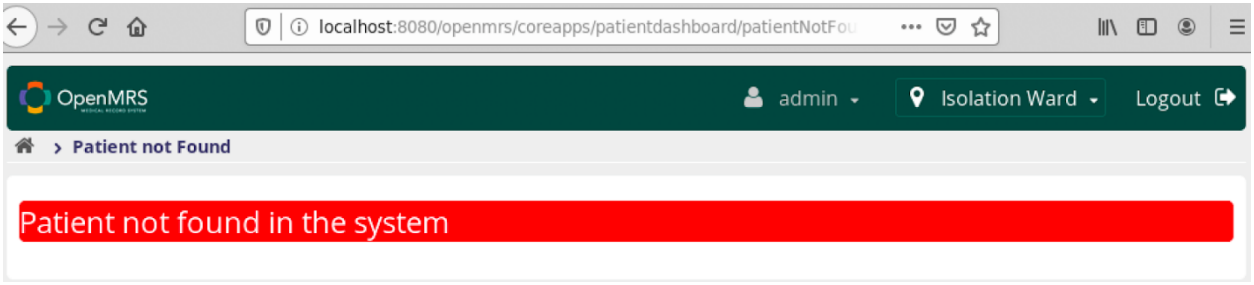
1. Login as admin by entering username as “admin” and password as “Admin123”.

2. Click on Find Patient Record
3. Open ‘John’s’ record. URL will be of the format - http://localhost:8080/openmrs/coreapps/clinicianfacing/patient.page?patientId=e117935d-2c04-11ea-a8c6-005056065e96
4. Modify the URL - http://localhost:8080/openmrs/coreapps/clinicianfacing/patient.page?patientId=1234567

Actual result:
Displays patient record not found.

Expected Result:
Should give appropriate error information without giving details about the error.

Result:
Passed



Test Case 6:

Test Case	ASVS	Unique ID	CWE
6	5.3.3	5.3.3-1	79

ASVS 5.3.3:

Verify that context-aware, preferably automated - or at worst, manual – output escaping protects against reflected, stored, and DOM based XSS.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Repeatable Steps:

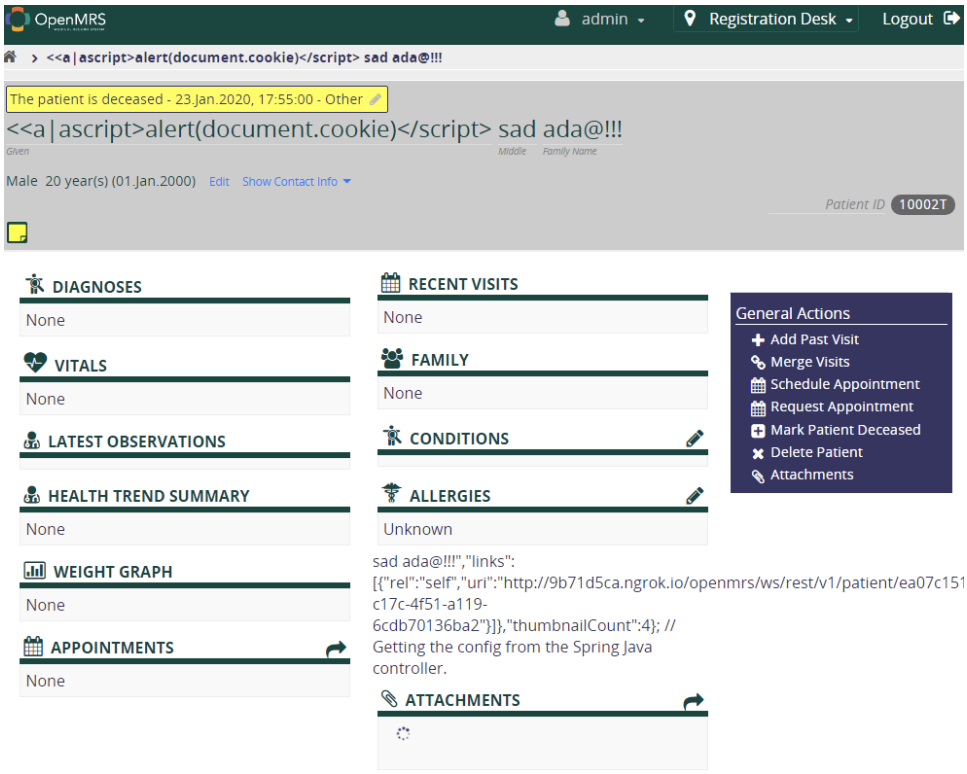
1. Login as admin by entering username as “admin” and password as “Admin123”.
2. Click on register a patient.
3. Enter the given name as <script>alert(document.cookie)</script>
4. Enter the middle name as “sad”
5. Enter the family name as ada@!!!
6. Select Gender & enter birthdate – Day -1; Month – January; Year -2000
7. Enter phone number as)(

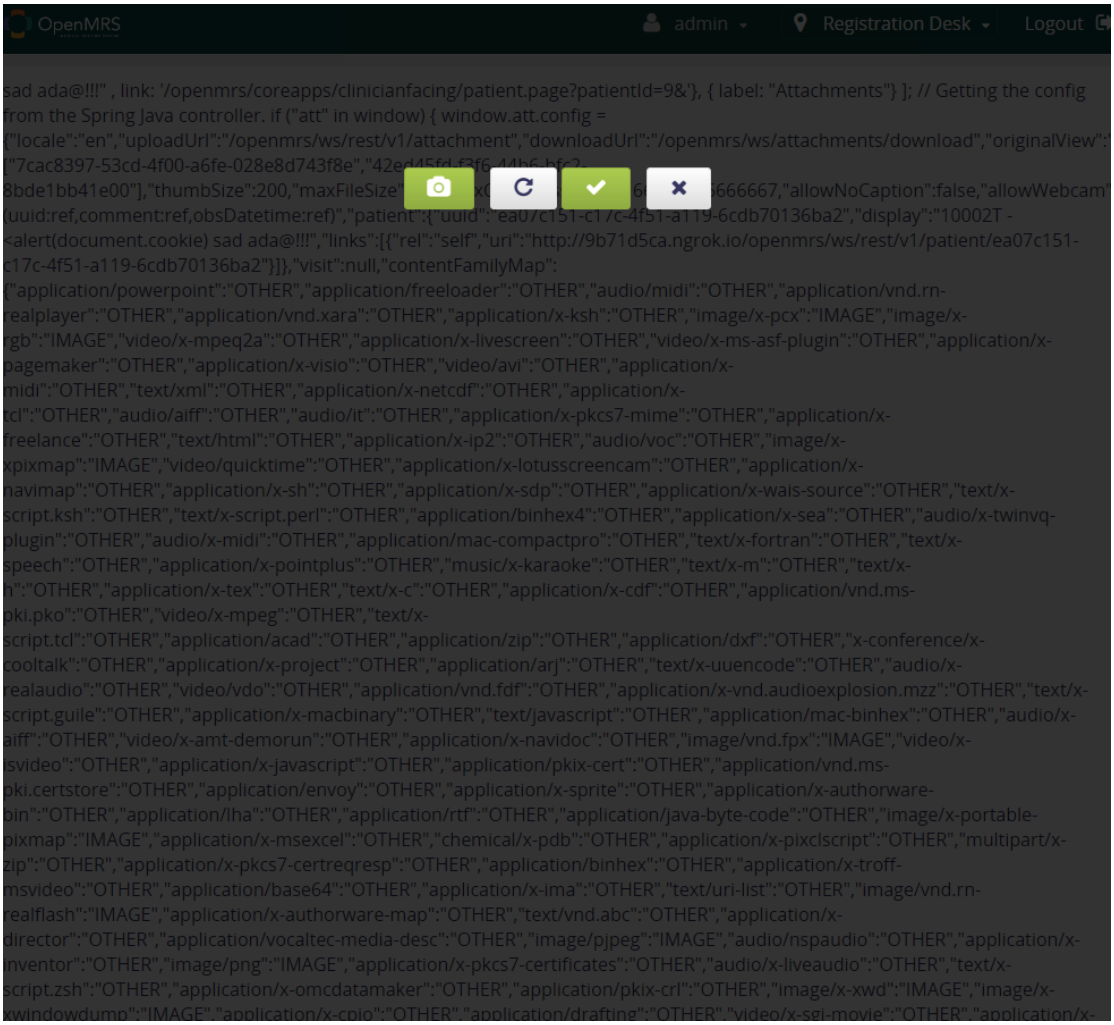
Actual result:

The server accepts the name with <script> Tag.

Expected result: The system should not allow <script> tag or any other tags to be stored in the database and should display an error for the same.

Result: Failed


OpenMRS
admin
Registration Desk
Logout
<<a|ascript>alert(document.cookie)</script> sad ada@!!!
The patient is deceased - 23.Jan.2020, 17:55:00 - Other
<<a|ascript>alert(document.cookie)</script> sad ada@!!!
Given
Middle
Family Name
Male 20 year(s) (01.Jan.2000) Edit Show Contact Info
Patient ID 10002T
DIAGNOSES
None
VITALS
None
LATEST OBSERVATIONS
HEALTH TREND SUMMARY
None
WEIGHT GRAPH
None
APPOINTMENTS
None
RECENT VISITS
None
FAMILY
None
CONDITIONS
ALLERGIES
Unknown
sad ada@!!!","links":
[{"rel":"self","uri":"http://9b71d5ca.ngrok.io/openmrs/ws/rest/v1/patient/ea07c151
c17c-4f51-a119-
6cdb70136ba2"}]},"thumbnailCount":4}; //
Getting the config from the Spring Java
controller.
ATTACHMENTS
General Actions
Add Past Visit
Merge Visits
Schedule Appointment
Request Appointment
Mark Patient Deceased
Delete Patient
Attachments



Test Case 7:

Test Case	ASVS	Unique ID	CWE
7	4.2.1	4.2.1-1	639

ASVS 4.2.1:

Verify that sensitive data and APIs are protected against direct object attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.

CWE Authorization Bypass Through User-Controlled Key:

The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

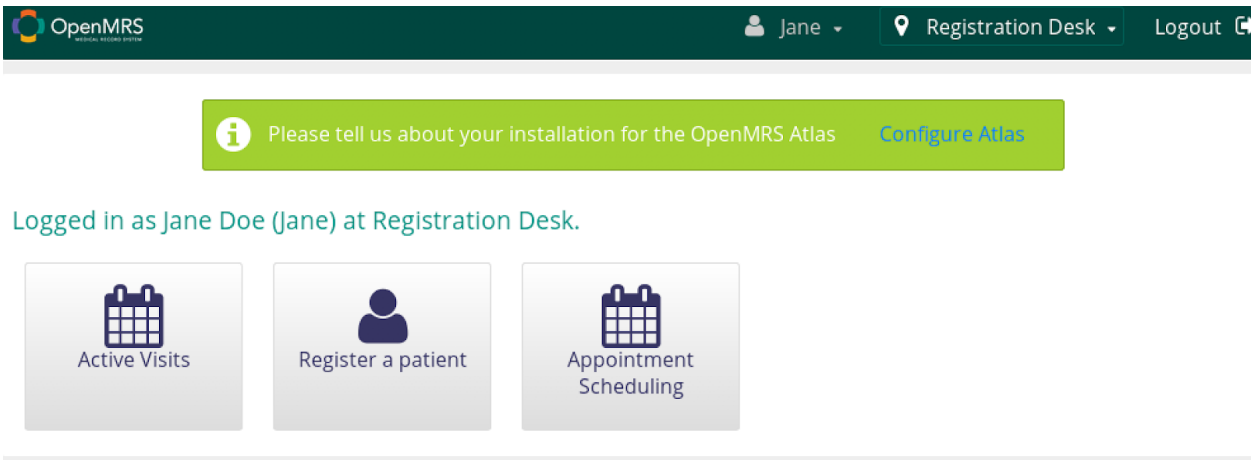
Repeatable steps:

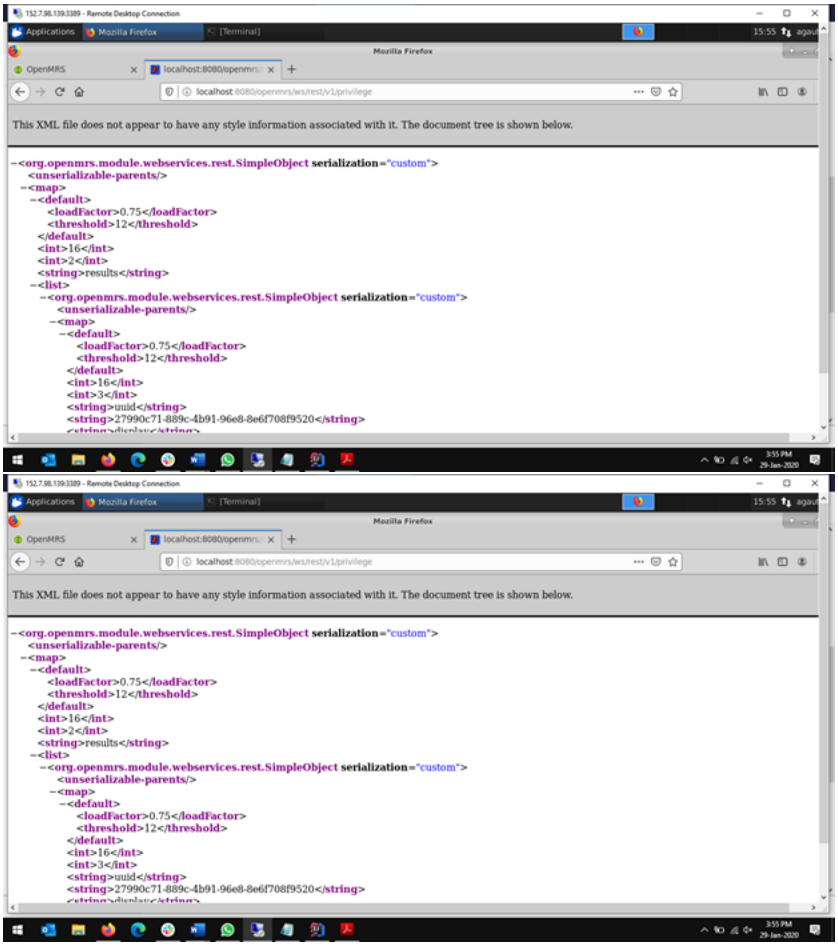
1. Login as admin by entering username as “admin” and password as “Admin123”.
2. Click on System Administration and then Advanced Administration to get API call for privilege - http://localhost:8080/openmrs/ws/rest/v1/privilege
3. This gives the details about the privileges.
4. Logout.
5. Login as registration Clerk
6. Type the same URL mentioned above mentioned in step 7.

Actual Results:
This displays all the results

Expected results:
Results should not be displayed since the user doesn’t have the access.

Result: Failed





Test case 8:

Test Case	ASVS	Unique ID	CWE
8	14.3.1	14.3.1-1	209

ASVS 14.3.1:

Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures

CWE 209 : Information Exposure Through an Error Message

The software generates an error message that includes sensitive information about its environment, users, or associated data.

Repeatable steps:

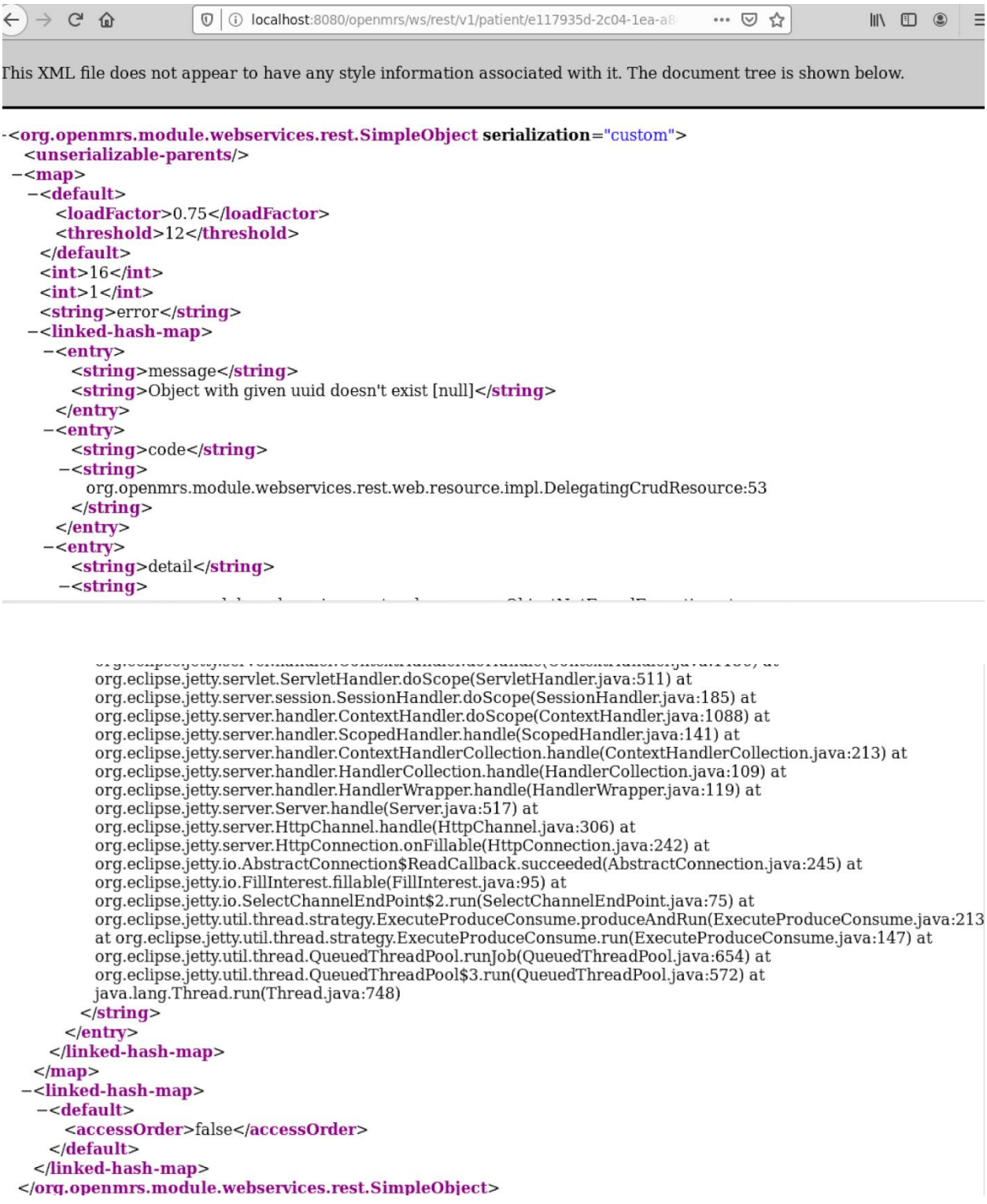
1. Login as admin by entering username as “admin” and password as “Admin123”.

2. Go to System Administration
3. Find patient - get the patient ID - e117935d-2c04-1iea-a8c6-005056065e96
4. Navigate to the home page.
5. Click on System Administration and then Advanced Administration.
6. Click on Api documentation to get the “find patient” API call
7. Get the API call and append patient ID - http://localhost:8080/openmrs/ws/rest/v1/patient/e117935d-2c04-1ea-a8c6-005056065e9
   This gives the details about the patient.
8. Modify the URL: http://localhost:8080/openmrs/ws/rest/v1/patient/e117935d-2c04-1ea-a8c6-123456

Actual Results:
Gives the complete stack trace:

Expected results:
Error details should not be displayed.

Result: Failed


localhost:8080/openmrs/ws/rest/v1/patient/e117935d-2c04-1ea-a8
This XML file does not appear to have any style information associated with it. The document tree is shown below.
-<org.openmrs.module.webservices.rest.SimpleObject serialization="custom">
<unserializable-parents/>
-<map>
-<default>
<loadFactor>0.75</loadFactor>
<threshold>12</threshold>
</default>
<int>16</int>
<int>1</int>
<string>error</string>
-<linked-hash-map>
-<entry>
<string>message</string>
<string>Object with given uuid doesn't exist [null]</string>
</entry>
-<entry>
<string>code</string>
-<string>
org.openmrs.module.webservices.rest.web.resource.impl.DelegatingCrudResource:53
</string>
</entry>
-<entry>
<string>detail</string>
-<string>
org.eclipse.jetty.servlet.ServletHandler.doScope(ServletHandler.java:511) at
org.eclipse.jetty.server.session.SessionHandler.doScope(SessionHandler.java:185) at
org.eclipse.jetty.server.handler.ContextHandler.doScope(ContextHandler.java:1088) at
org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:141) at
org.eclipse.jetty.server.handler.ContextHandlerCollection.handle(ContextHandlerCollection.java:213) at
org.eclipse.jetty.server.handler.HandlerCollection.handle(HandlerCollection.java:109) at
org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.java:119) at
org.eclipse.jetty.server.Server.handle(Server.java:517) at
org.eclipse.jetty.server.HttpChannel.handle(HttpChannel.java:306) at
org.eclipse.jetty.server.HttpConnection.onFillable(HttpConnection.java:242) at
org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection.java:245) at
org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:95) at
org.eclipse.jetty.io.SelectChannelEndPoint$2.run(SelectChannelEndPoint.java:75) at
org.eclipse.jetty.util.thread.strategy.ExecuteProduceConsume.produceAndRun(ExecuteProduceConsume.java:213
at org.eclipse.jetty.util.thread.strategy.ExecuteProduceConsume.run(ExecuteProduceConsume.java:147) at
org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:654) at
org.eclipse.jetty.util.thread.QueuedThreadPool$3.run(QueuedThreadPool.java:572) at
java.lang.Thread.run(Thread.java:748)
</string>
</entry>
</linked-hash-map>
</map>
-<linked-hash-map>
-<default>
<accessOrder>false</accessOrder>
</default>
</linked-hash-map>
</org.openmrs.module.webservices.rest.SimpleObject>

org.openmrs.web.filter.StartupFilter.doFilter(StartupFilter.java:105) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1669) at
org.openmrs.web.filter.StartupFilter.doFilter(StartupFilter.java:105) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1669) at
org.openmrs.web.filter.StartupFilter.doFilter(StartupFilter.java:105) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1669) at
org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:88) at
org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:107) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1669) at
org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:581) at
org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:143) at
org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:548) at
org.eclipse.jetty.server.session.SessionHandler.doHandle(SessionHandler.java:226) at
org.eclipse.jetty.server.handler.ContextHandler.doHandle(ContextHandler.java:1156) at
org.eclipse.jetty.servlet.ServletHandler.doScope(ServletHandler.java:511) at
org.eclipse.jetty.server.session.SessionHandler.doScope(SessionHandler.java:185) at
org.eclipse.jetty.server.handler.ContextHandler.doScope(ContextHandler.java:1088) at
org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:141) at
org.eclipse.jetty.server.handler.ContextHandlerCollection.handle(ContextHandlerCollection.java:213) at
org.eclipse.jetty.server.handler.HandlerCollection.handle(HandlerCollection.java:109) at
org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.java:119) at
org.eclipse.jetty.server.Server.handle(Server.java:517) at
org.eclipse.jetty.server.HttpChannel.handle(HttpChannel.java:306) at
org.eclipse.jetty.server.HttpConnection.onFillable(HttpConnection.java:242) at
org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection.java:245) at
org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:95) at
org.eclipse.jetty.io.SelectChannelEndPoint$2.run(SelectChannelEndPoint.java:75) at
org.eclipse.jetty.util.thread.strategy.ExecuteProduceConsume.produceAndRun(ExecuteProduceConsume.java:213
at org.eclipse.jetty.util.thread.strategy.ExecuteProduceConsume.run(ExecuteProduceConsume.java:147) at
org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:654) at

</string>
</entry>
−<entry>
<string>detail</string>
−<string>
org.openmrs.module.webservices.rest.web.response.ObjectNotFoundException at
org.openmrs.module.webservices.rest.web.resource.impl.DelegatingCrudResource.retrieve(DelegatingCrudResou
at
org.openmrs.module.webservices.rest.web.v1_0.controller.MainResourceController.retrieve(MainResourceContr
at sun.reflect.GeneratedMethodAccessor1026.invoke(Unknown Source) at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at
java.lang.reflect.Method.invoke(Method.java:498) at
org.springframework.web.bind.annotation.support.HandlerMethodInvoker.invokeHandlerMethod(HandlerMetho
at
org.springframework.web.servlet.mvc.annotation.AnnotationMethodHandlerAdapter.invokeHandlerMethod(Anne
at
org.springframework.web.servlet.mvc.annotation.AnnotationMethodHandlerAdapter.handle(AnnotationMethodH
at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:943) at
org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:877) at
org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:966) at
org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:857) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:687) at
org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:842) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:790) at
org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:816) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1686) at
org.openmrs.module.web.filter.ForcePasswordChangeFilter.doFilter(ForcePasswordChangeFilter.java:60) at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1669) at
org.openmrs.module.web.filter.ModuleFilterChain.doFilter(ModuleFilterChain.java:72) at
org.openmrs.web.filter.GZIPFilter.doFilterInternal(GZIPFilter.java:64) at

Test case 9 :

Test Case	ASVS	Unique ID	CWE
9	2.2.1	2.2.1-1	307

ASVS 2.2.1:
Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

CWE 307: **Improper Restriction of Excessive Authentication Attempts**
The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.

Repeatable steps:
1. login to the user account with a wrong password
2. the system does not login
3. continue to type the wrong password again , and keep repeating it

Actual result :
The account was locked after 8th attempt

Expected result:
The account should be locked after a few failed attempt

Result :
PASSED

Test case 10:

Test Case	ASVS	Unique ID	CWE
10	2.5.4	2.5.4-1	16

ASVS 2.5.4:
Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").

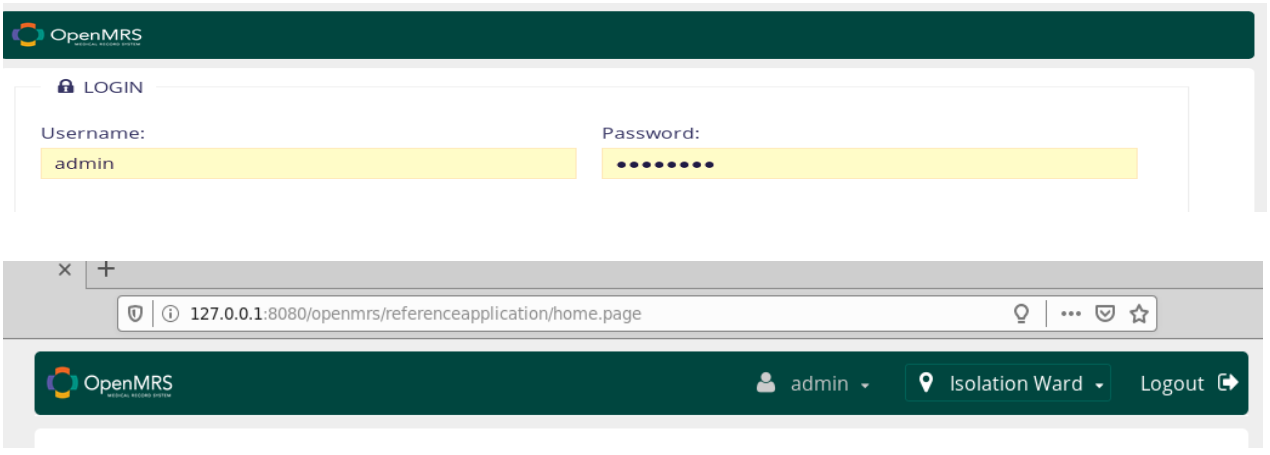
CWE 16: Configuration
Weaknesses in this category are typically introduced during the configuration of the software.

Repeatable steps:
1. go to the login page
2. try to login with ‘admin’ user and password ‘Admin123’

Actual result:
The system logs in with the admin account

Expected Result :
There should not ne any ‘admin’ account or any other default account

Result :
FAILED



Test case 11 :

Test Case	ASVS	Unique ID	CWE

11	2.5.2	2.5.2-1	640

ASVS 2.5.2:
Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.

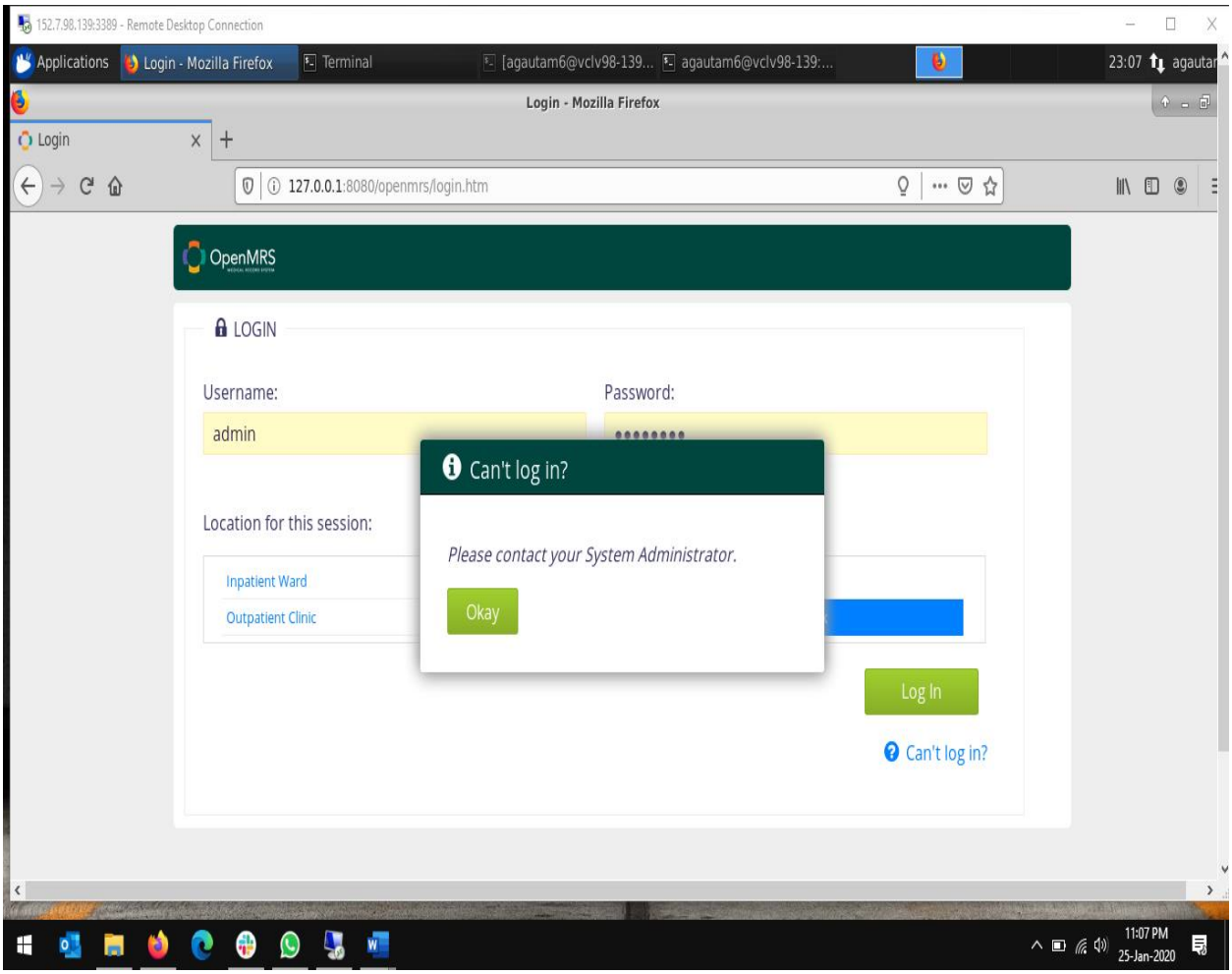
CWE 640: **Weak Password Recovery Mechanism for Forgotten Password**
The software contains a mechanism for users to recover or change their passwords without knowing the original password, but the mechanism is weak.

Repeatable steps:
1. go to the OpenMRS login page
2. type in the username as ‘admin’
3. click on ‘Can’t Log In’

Actual result:
The system notifies to contact the system administrator

Expected result:
There should be no hints or knowledge-based authentication

Result : PASSED



Test case 12 :

Test Case	ASVS	Unique ID	CWE
12	9.1.1	9.1.1-1	319

ASVS 9.1.1:
Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.

CWE 319: Cleartext Transmission of Sensitive Information
The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

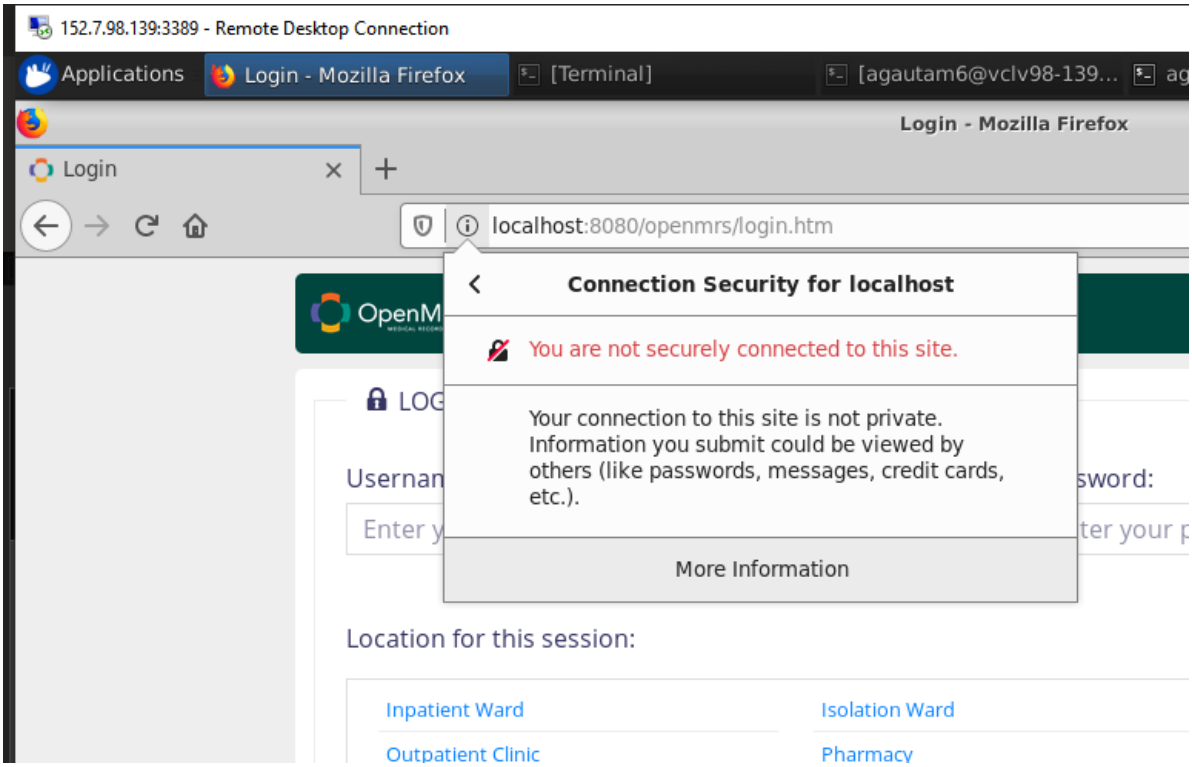
Repeatable steps:

1. open the browser
2. type the following in the URL bar : http://127.0.01:8080/openmrs

Actual result:
The webpage shows up with no TLS / SSL enabled

Expecetd result:
the webpage should open up with TLS/SSL enabled or should deny the request

Result: FAILED



Test case 13 :

Test Case	ASVS	Unique ID	CWE
13	10.2.2	10.2.2-1	272

ASVS 10.2.2 :
Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.

CWE 272: Least Privilege Violation
The elevated privilege level required to perform operations such as chroot() should be dropped immediately after the operation is performed.

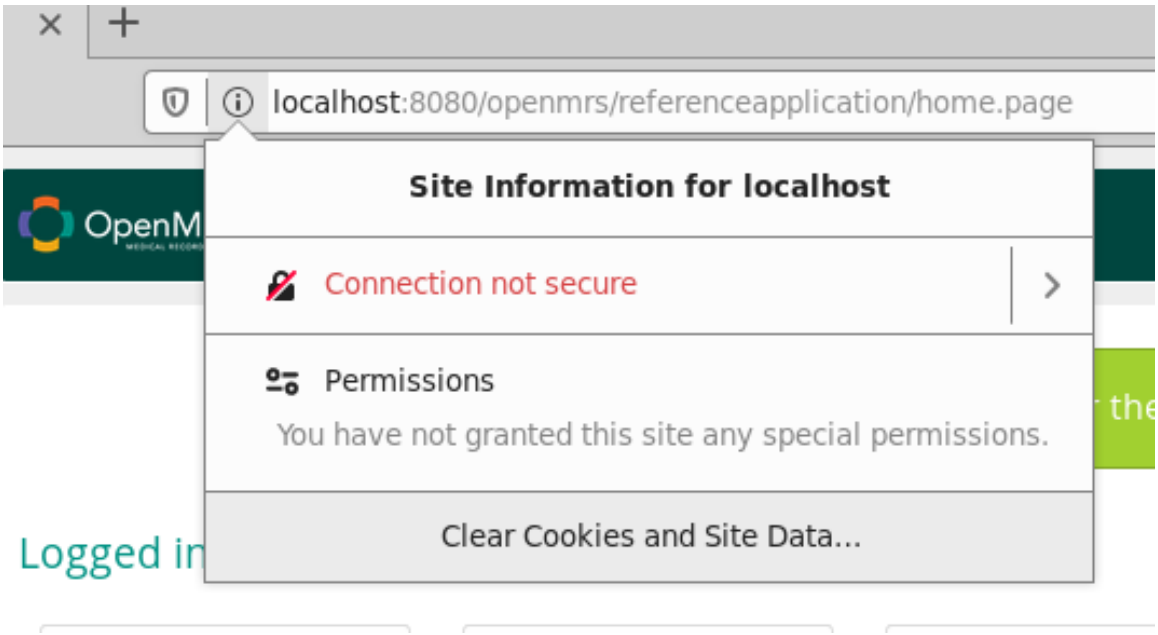
Repeatable steps:

1. open firefox (or any browser in which you are using the OpenMRS application)
2. click on the ‘i’ icon near the URL
3. observe the permissions tab

Actual result:
It clearly states ‘ you have not granted any special permissions to this site’

Expected result: the application does not ask for any special permission

Result : PASSED



Test case 14 :

Test Case	ASVS	Unique ID	CWE
14	4.1.3	4.1.3-1	285

ASVS 4.1.3 :
Verify that the principle of least privilege exists -users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.

CWE 285: Improper Authorization
The software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

Repeatable steps:

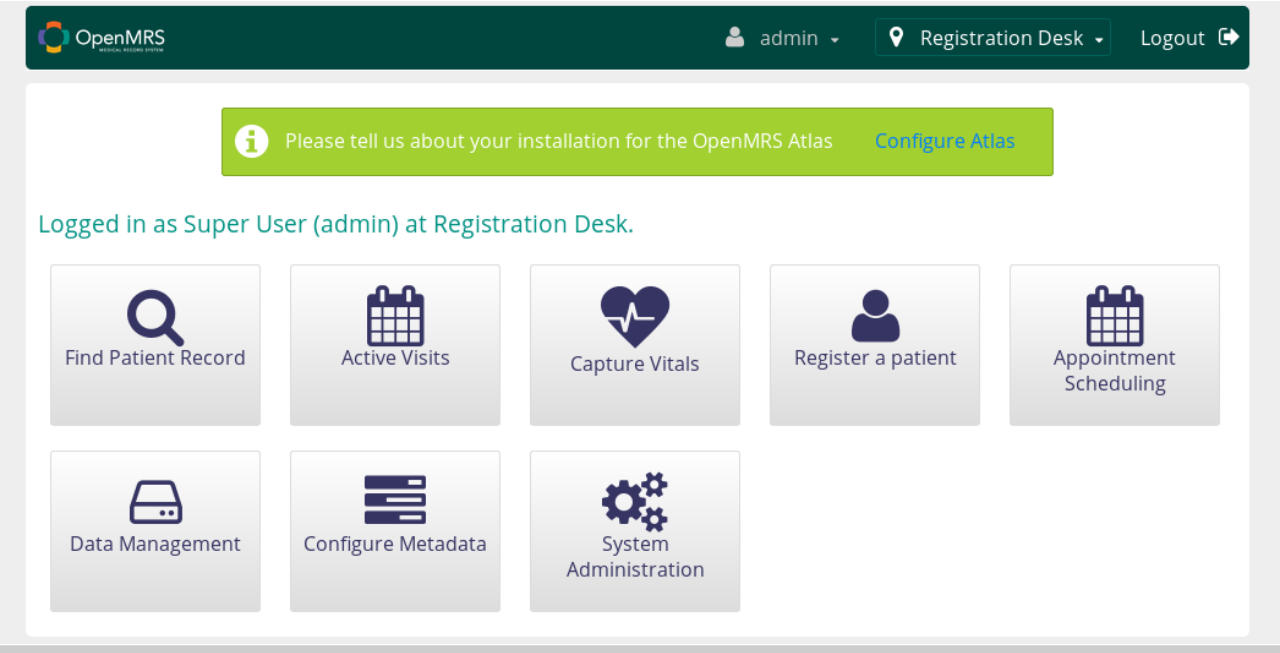
1. login to OpenMRS as ‘admin’ user and password as ‘Admin123’
2. logout of the admin user
3. login to OpenMrs as user ‘putin123’ and password ‘Ab123456’

Expected result:
The views should be different for admin user and for other user roles

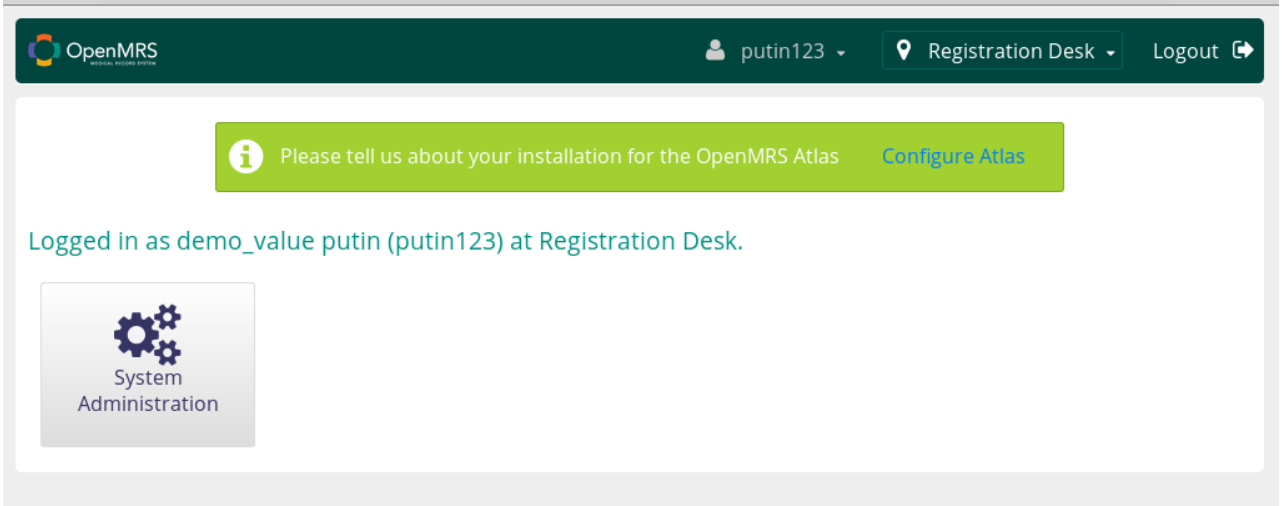
Actual result :
The views are different for other users and admin users

Result :
PASSED

Admin user view:



Putin123 user view:



Test case 15 :

Test Case	ASVS	Unique ID	CWE
15	11.1.8	11.1.8-1	390

ASVS 11.1.8:
Verify the application has configurable alerting when automated attacks or unusual activity is detected.

CWE 390: **Detection of Error Condition Without Action**
The software detects a specific error, but takes no actions to handle the error.

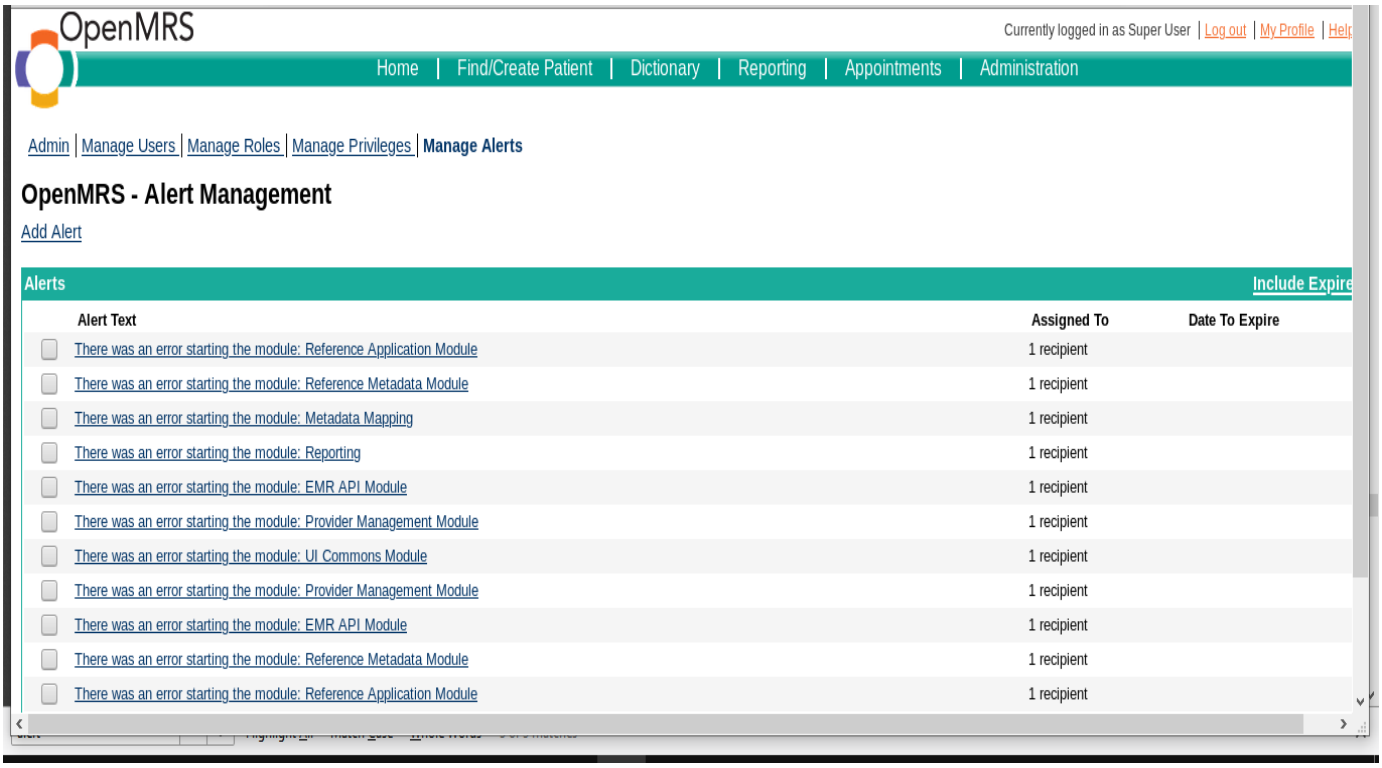
Repeatable steps:

1. Login using the user ‘admin’ and password ‘Admin123’
2. Click on ‘System Administration’
3. Click on ‘Advanced Administration’
4. Click on ‘Manage Alerts’

Expected Result:
a configurable alert window should be shown and unusual activity should be reported

Actual result:
a configurable alert window is shown and unusual activity is being reported

Result:
Passed



Test Case 16:

Find Patient record - SQL injection

Test case	ASVS	Unique ID	CWE
1.1	5.3.4	5.3.4-2	89

ASVS 5.3.4: Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks

CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
The software constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or

incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

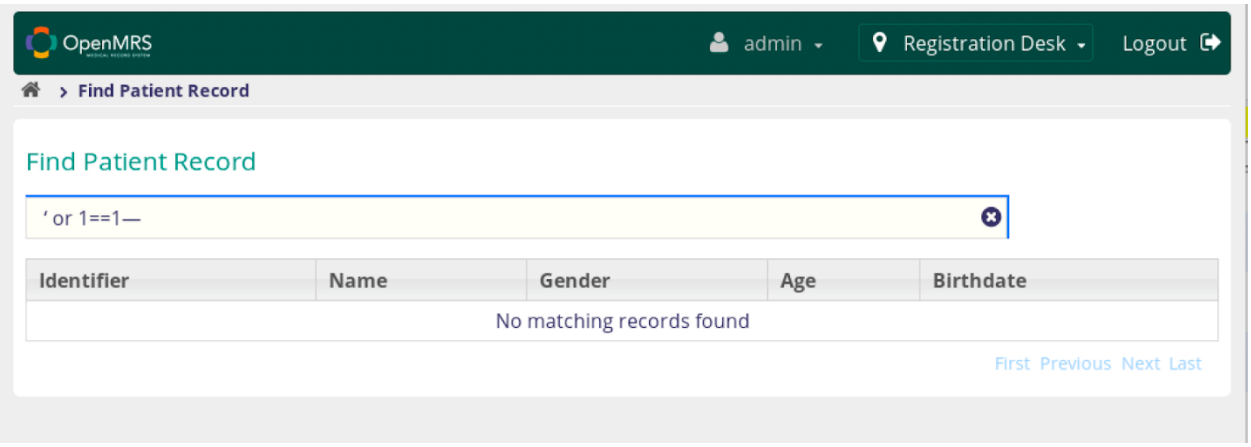
Repeatable steps:

1. Login as admin by entering username as “admin” and password as “Admin123”.
2. Click on find patient record.
3. Type “‘ or 1==1-- “ in the search field.

Actual Result:
Displays no matching record

Expected Result:
Should display any patient details

Result:
Passed



Time based Metric for Black Box Testing:

Test cases carried out per hour: 3 test cases per hour (approximately)

Total time taken for Black Box testing: 5 hours 30 minutes (approximately)

Fortify Reports

1)

Module	RESULT	ASVS	CWE
Appointmentscheduling	True Positive	5.1.3	20

- **Issue:** Cross-Site Scripting
  Input validation and representation issue in appointments.jsp page. The user input is stored in the variable, patientId on line 17 as per the screenshot attached which is passed into a web address without a sanity check of the input. Hence, this can be considered as a potential True positive result. This vulnerability could result in phishing attacks, browser executing malicious code, allow unvalidated input to control the URL.

appointments.jsp, line 18 (Cross-Site Scripting: DOM)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The method addNewAppointment() in appointments.jsp sends unvalidated data to a web browser on line 18, which can result in the browser executing malicious code.		

Source: appointments.jsp:17 Read value()

```
15    //Navigate to appointmentForm.form
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
```

Sink: appointments.jsp:18 Assignment to window.location()

```
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
20    //On the page load updates necessary stuff
```

- Explain how to fix the vulnerability
  Validation occurs at the correct places and checks are made for the correct properties.

2)

Module	RESULT	ASVS	CWE
Appointmentscheduling	False Positive	-	-

- **Issue: Key Management: Hardcoded Encryption Key**

The security fault highlighted below treats the key as an encryption key. Declaring a variable name as a key, does not mean its functioning will be dependent on its name, hence it is identified as a false positive.

jquery.jeditable.js, line 515 (Key Management: Hardcoded Encryption Key)			
Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Security Features		
Abstract:	Hardcoded encryption keys can compromise security in a way that cannot be easily remedied.		
Sink:	jquery.jeditable.js:515 Operation()		

```
513                 continue;
514             }
515             if ('selected' == key) {
516                 continue;
517             }
```

3)

Module	RESULT	ASVS	CWE
calculation	True Positive	5.1.3	20

- **Issue: Header Manipulation : Cookies**
  Cookie information is being created based on the input from the URL. A user can make changes in the web address which is being used as an input in the sName variable field in line 3697. This vulnerability can be exploited to carry out cross-site scripting, page hijacking or cache-poisoning attacks.

jquery.dataTables.js, line 3699 (Header Manipulation: Cookies)			
Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method _fnCreateCookie() in jquery.dataTables.js includes unvalidated data in an HTTP cookie on line 3699. This enables Cookie manipulation attacks and can lead to other HTTP Response header manipulation attacks like: cache-poisoning, cross-site scripting, cross-user defacement, page hijacking or open redirect.		
Source:	jquery.dataTables.js:3697 Read window.location()		

```
3695             * have to append the pathname to the cookie name. Appalling.
3696             */
3697            sName += '_'+window.location.pathname.replace(/[\/:]/g,"").toLowerCase();
3698
3699            document.cookie = sName+"="+sValue+"; expires="+date.toGMTString()+"; path=/";
```

Sink: jquery.dataTables.js:3699 Assignment to document.cookie()

```
3697            sName += '_'+window.location.pathname.replace(/[\/:]/g,"").toLowerCase();
3698
3699            document.cookie = sName+"="+sValue+"; expires="+date.toGMTString()+"; path=/";
3700        }
3701
```

- Explain how to fix the vulnerability
  Validate data immediately before it leaves the application. Perform input validation for Header Manipulation. Create a whitelist of safe characters which is allowed to be present in the response headers and validate user input based on the whitelist.

4) Module:

Module	RESULT	ASVS	CWE
reportingCompatibility	False Positive	-	-

- **Issue: Log Forging**
  As stated in the screenshot below, the CohortSearchHistory.java writes unvalidated user input to the log on line 404. However, value of the temp variable, which takes in the user input is not being added to the log. It is true that the temp value is not sanitized but the value being appended to the log error is description, which has not been defined as per the information stated. Hence, this issue can be stated as a False Positive.

CohortSearchHistory.java, line 404 (Log Forging)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method createCompositionFilter() in CohortSearchHistory.java writes unvalidated user input to the log on line 404. An attacker could take advantage of this behavior to forge log entries or inject malicious content into the log.		

Source: CohortBuilderController.java:403 javax.servlet.ServletRequest.getParameter()

```
401     log.warn("addCohort(id) didn't find " + cohortId);
402   }
403   temp = request.getParameter("composition");
404   if (temp != null) {
405    PatientSearch ps = history.createCompositionFilter(temp);
```

Sink: CohortSearchHistory.java:404 org.apache.commons.logging.Log.error()

```
402   }
403   catch (Exception ex) {
404    log.error("Error in description string: " + description, ex);
405    return null;
406   }
```

5)

Module	RESULT	ASVS	CWE
uiframework	True Positive	5.1.3	20

Issue: Path Manipulation
The file system path is vulnerable to attack from the user input as it is not validated at any point of time. The path variable takes in the value from the input field as per line 94 in the

diagram and then directly adds the path to the file as shown in line 45. The attacker could possibly exploit this vulnerability and carry out potential file path changes.

ModuleResourceProvider.java, line 45 (Path Manipulation)			
Fortify Priority:	Critical	Folder	Critical
Kingdom:	Input Validation and Representation		
Abstract:	Attackers are able to control the file system path argument to File() at ModuleResourceProvider.java line 45, which allows them to access or modify otherwise protected files.		

Source: ResourceServlet.java:94 javax.servlet.http.HttpServletRequest.getPathInfo()

```
92    ResourceFactory factory = ResourceFactory.getInstance();
93
94    String path = request.getPathInfo();
95    try {
96     // path is like "/uiframework/resource/providerName/path/to/resource.png"
```

Sink: ModuleResourceProvider.java:45 java.io.File.File()

```
43     for (File developmentFolder : developmentFolders) {
44         // we're in development mode, and we want to dynamically reload resource from this
filesystem directory
45       File file = new File(developmentFolder, path);
46       if (file.exists()) {
47        return file;
```

- Explain how to fix the vulnerability
  The vulnerability can be fixed by sanitizing the input. Proper input validation is required and data verification at the back end would help to lower the possible exposure the site has provided.

6)

Module	RESULT	ASVS	CWE
adminuni	False Positive	-	-

Issue: Password Management: Password in Configuration File
The following is a False Positive alert because the password mentioned in this context "adminuni.myAccount.password.label", is an identifier not a hardcoded password. Hence, this would not compromise the system.

messages.properties, line 75 (Password Management: Password in Configuration File)			
Fortify Priority:	High	Folder	High
Kingdom:	Environment		
Abstract:	Storing a plain text password in a configuration file may result in a system compromise.		

Sink: messages.properties:75 adminui.myAccount.password.label()

```
73  adminui.myAccount=My Account
74  adminui.myAccount.myLanguages.title=My Languages
75  adminui.myAccount.password.label=Password
76  adminui.myAccount.changeSecretQuestion.label=Secret Question
77  adminui.myAccount.defaults.label=User Defaults
```

7)

Module	RESULT	ASVS	CWE
adminuni	False Positive	-	-

Issue: Password Management: Hardcoded Password

The forcePassword is acting as a flag and the system security is not affected in any way. The password is not being hardcoded here.

userDetails.js, line 139 (Password Management: Hardcoded Password)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	Hardcoded passwords may compromise system security in a way that cannot be easily remedied.		

Sink: userDetails.js:139 FieldAccess: forcePassword()

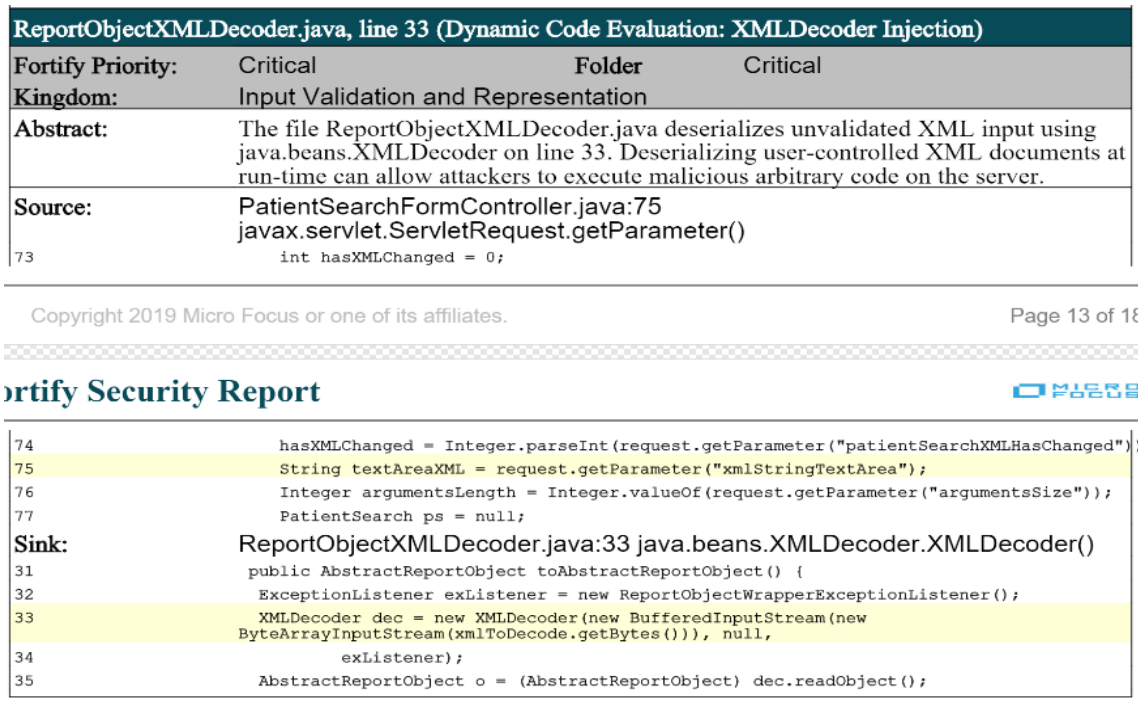
```
137                 var uProperties = {};
138                 if(modelUser.userProperties.forcePassword){
139                     uProperties.forcePassword =******
140                 }
141                 angular.forEach(modelUser.userProperties, function(value, key) {
```

8)

Module	RESULT	ASVS	CWE
reportingcompatibility	True Positive	5.5.3	502

Issue: Dynamic Code Evaluation: XMLDecoder Injection

XMLDecoder injection. Deserializing user-controlled XML documents at run-time can allow attackers to execute malicious arbitrary code on the server.



ReportObjectXMLDecoder.java, line 33 (Dynamic Code Evaluation: XMLDecoder Injection)			
Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file ReportObjectXMLDecoder.java deserializes unvalidated XML input using java.beans.XMLDecoder on line 33. Deserializing user-controlled XML documents at run-time can allow attackers to execute malicious arbitrary code on the server.		
Source:	PatientSearchFormController.java:75 javax.servlet.ServletRequest.getParameter()		

```
73          int hasXMLChanged = 0;
```



```
74          hasXMLChanged = Integer.parseInt(request.getParameter("patientSearchXMLHasChanged"));
75          String textAreaXML = request.getParameter("xmlStringTextArea");
76          Integer argumentsLength = Integer.valueOf(request.getParameter("argumentsSize"));
77          PatientSearch ps = null;
```

Sink: ReportObjectXMLDecoder.java:33 java.beans.XMLDecoder.XMLDecoder()

```
31   public AbstractReportObject toAbstractReportObject() {
32    ExceptionListener exListener = new ReportObjectWrapperExceptionListener();
33    XMLDecoder dec = new XMLDecoder(new BufferedInputStream(new
ByteArrayInputStream(xmlToDecode.getBytes())), null,
34            exListener);
35    AbstractReportObject o = (AbstractReportObject) dec.readObject();
```

- Explain how to fix the vulnerability
  The vulnerability can be fixed by sanitizing the user input. Proper input validation is required and data verification at the back end would help to lower the possible exposure the site has provided. Some Java packages can be used to verify the input such as Validator, SchemaFactory, etc.

9)

Module	RESULT	ASVS	CWE
reportingcompatibility	True Positive	11.1.6	367

Issue: Race Condition: Singleton Member Field
The class IdentifierBuilder is a singleton, which can result in a member field accessing the shared data between users. This can be exploited by an attacker to view another user's data. Storing user data in Servlet member fields introduces a data access race condition.

IdentifierBuilder.java, line 80 (Race Condition: Singleton Member Field)			
Fortify Priority:	High	**Folder**	High
Kingdom:	Time and State		
Abstract:	The class IdentifierBuilder is a singleton, so the member field iss is shared between users. The result is that one user could see another user's data.		
Sink:	IdentifierBuilder.java:80 AssignmentStatement()		

```
78      private IdentifierSourceService getIss() {
79          if (iss == null) {
80              iss = Context.getService(IdentifierSourceService.class);
81          }
82          return iss;
```

- Explain how to fix the vulnerability
  This vulnerability can be fixed if all the read write operations on the shared member field are run atomically on the same synchronized block.

10)

Module	RESULT	ASVS	CWE
owa	True Positive	14.4.1	173

Issue: Open Redirect
Unvalidated data is passed into a HTTP redirect function which can lead to redirection to unknown sites and creates a possibility of phishing attacks.

RedirectServlet.java, line 57 (Open Redirect)			
Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file RedirectServlet.java passes unvalidated data to an HTTP redirect function on line 57. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.		
Source:	RedirectServlet.java:54 javax.servlet.http.HttpServletRequest.getRequestURL()		

```
52      private void processRequest(HttpServletRequest request, HttpServletResponse response,
        boolean content)
53              throws IOException {
54        String url = request.getRequestURL().toString().replace("/ms/owa/redirectServlet",
        "/owa");
55        //@TODO redirecting to original url after login in openmrs.
56        String loginUrl = Context.getAdministrationService().getGlobalProperty("login.url",
        "login.htm");
```

Sink: RedirectServlet.java:57
javax.servlet.http.HttpServletResponse.sendRedirect()

```
55        //@TODO redirecting to original url after login in openmrs.
56        String loginUrl = Context.getAdministrationService().getGlobalProperty("login.url",
        "login.htm");
57        response.sendRedirect(request.getContextPath() + "/" + loginUrl + "?redirect=" + url);
58      }
59      }
```

- Explain how to fix the vulnerability
  The vulnerability can be fixed by creating a list of legitimate resource names that a user is allowed to specify, and allow the user to select from the list. Utilizing this approach, the input provided by the user is never used directly to specify the resource name.
  Maintaining a blacklist is also helpful.

Time based Metric for fortify:

Number of defects found per hour using fortify: 2 Defects per hour
Number of true-positives: 6 defects (3 hours approximately)
Total amount of time spent on analyzing fortify report: 5 hours (approximately)

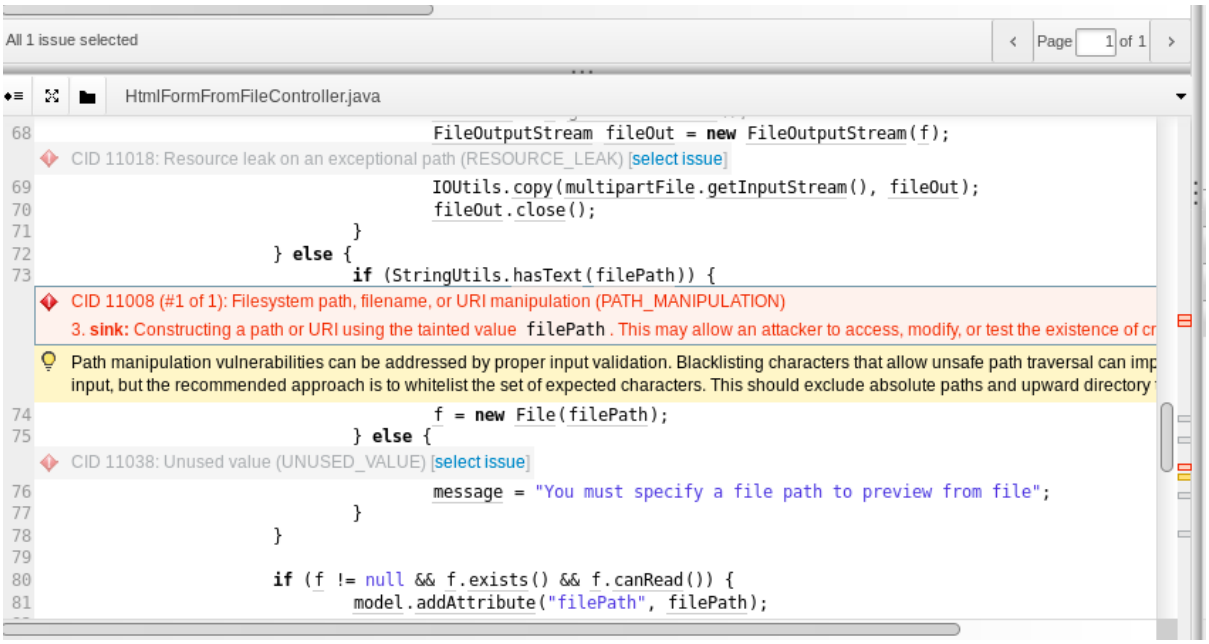
Coverity Report

1. **Module Name -** htmlformentry
   CID 11008: Filesystem path, filename, or URI manipulation (Path Manipulation)
   Category: High Impact Security
   ASVS 12.3.1:
   Verify that user-submitted filename metadata is not used directly with system or framework file and URL API to protect against path traversal.
   CWE: 22
   Vulnerability type: True positive

   Description:
   The variable 'filePath' is tainted because it comes from a HTTP request. Subsequently in the code, a path or URI is created using this parameter. This allows attackers to access, modify, or test the existence of critical or sensitive files.

   Vulnerability Fix:
   Path manipulation vulnerabilities can be addressed by appropriate input validation. Blacklisting characters that allow unsafe path traversal could improve the safety of the input, but the recommended approach is to whitelist the set of expected characters. This should exclude absolute paths and upward directory traversal

   Snapshot:



2. **Module Name** – htmlformentry
   CID 10996: SQL Injection
   Category: Medium Impact Security
   ASVS 5.3.4 :
   Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks
   CWE: 89
   Vulnerability type: True positive

   Description:

   The parameter ‘searchAttribute’ is tainted as it is one of the request params of the incoming HTTP request. In the function, getPersonIdHavingAttributes(), a SQL query statement is created using this param. As the SQL command string flows out of the function, it can be used to access the database elsewhere.

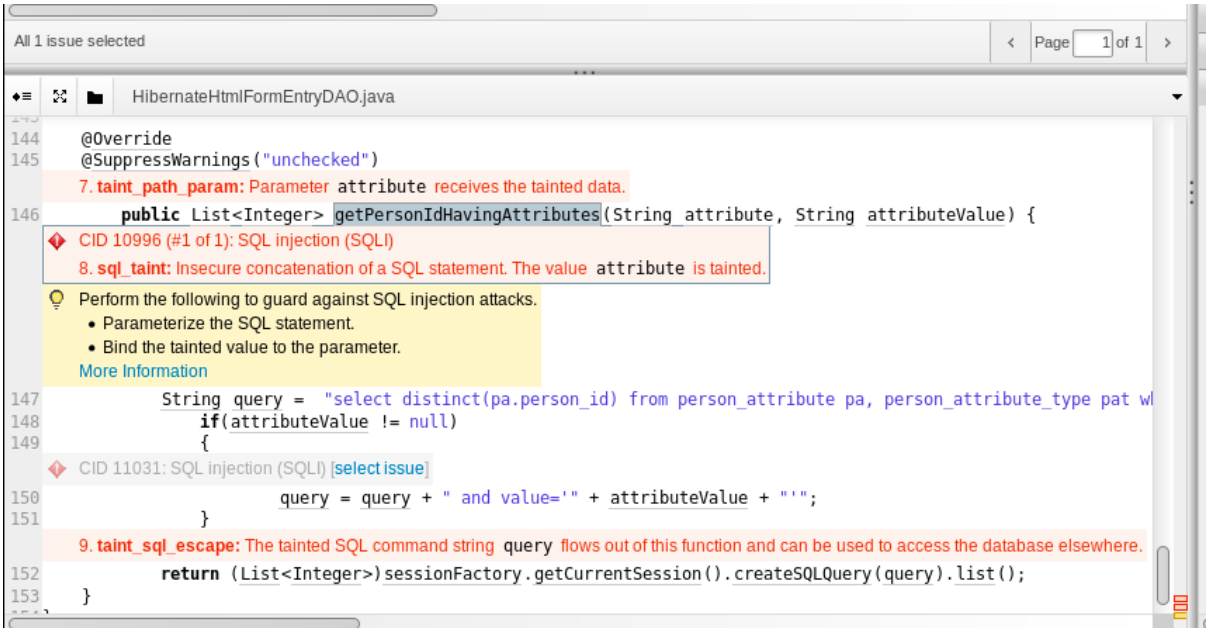
   Vulnerability Fix:

To remedy both SQL injection and preserve the meaning of the query, one could:
1.Parameterize the SQL statement.

2.Escape the percent sign (%, U+0025) and underscore (_, U+005F) characters within the string used in the LIKE query '%...%'.

3. Bind the value to a parameter within the LIKE clause.

Snapshot:



3. **Module Name** – addresshiearchy
   CID 10530: Open redirect
   Category: Medium Impact Security
   ASVS 5.1.5:
   Verify that URL redirects and forwards only allow whitelisted destinations, or show a warning when redirecting to potentially untrusted content.
   CWE: 601

Vulnerability type: True positive

Description:

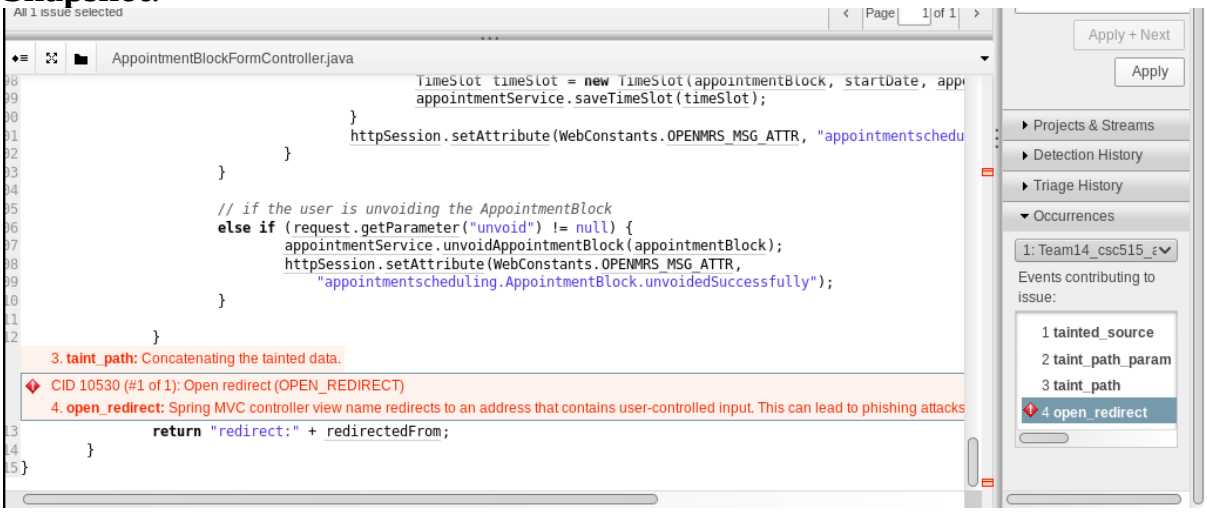
The request-param ‘redirectedForm’ is tainted because it comes from an HTTP request.The function in the end redirects to an address that contains the tainted param i.e the address contains user-controlled input. Such an exposure of the redirect url can lead to a potential phishing attack.

Vulnerability Fix:

1. Use an intermediate disclaimer page that provides the user with a clear warning that they are leaving the current site.

2. Ensure that no externally- supplied requests are honored by requiring that all redirect requests include a unique nonce generated by the application.

Snapshot:



4. **Module Name** – calculation
   CID 10576: Unsafe reflection
   Category: Low Impact Security

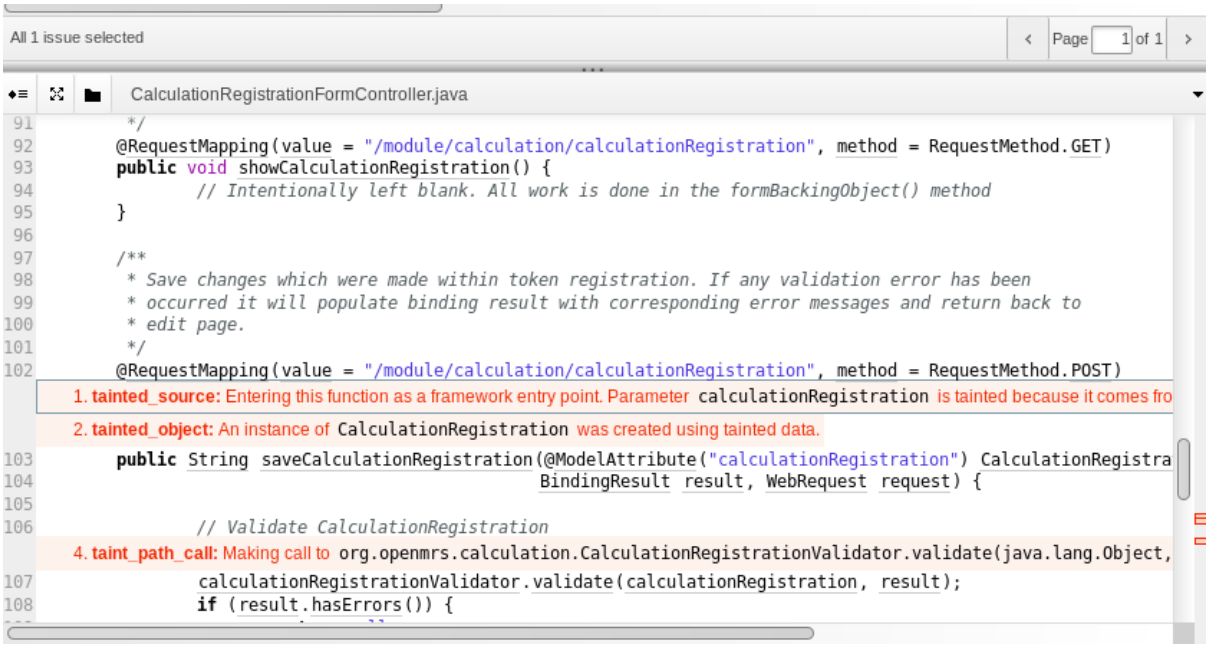
ASVS 1.4.3:
Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.
CWE: 470
Vulnerability type: True Positive

Description:
The model attribute 'calculationRegistration' is tainted because it comes from an HTTP request. Later, in function - getCalculation(),the value is passed to a reflection API. This may allow an attacker to bypass security checks, obtain unauthorized data, or execute arbitrary code. Also, the value is used unsafely in bytecode, which cannot be displayed.

Vulnerability Fix:

Validating tainted data against a limited set of static, trusted reflection classes, methods, or fields can fix this type of vulnerability.

Snapshot:



5. **Module Name** – coreapps
CID 10682: Unsafe deserialization

Category: High Impact Security
ASVS 5.5.1:
Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering
CWE: 502
Vulnerability type:True Positive

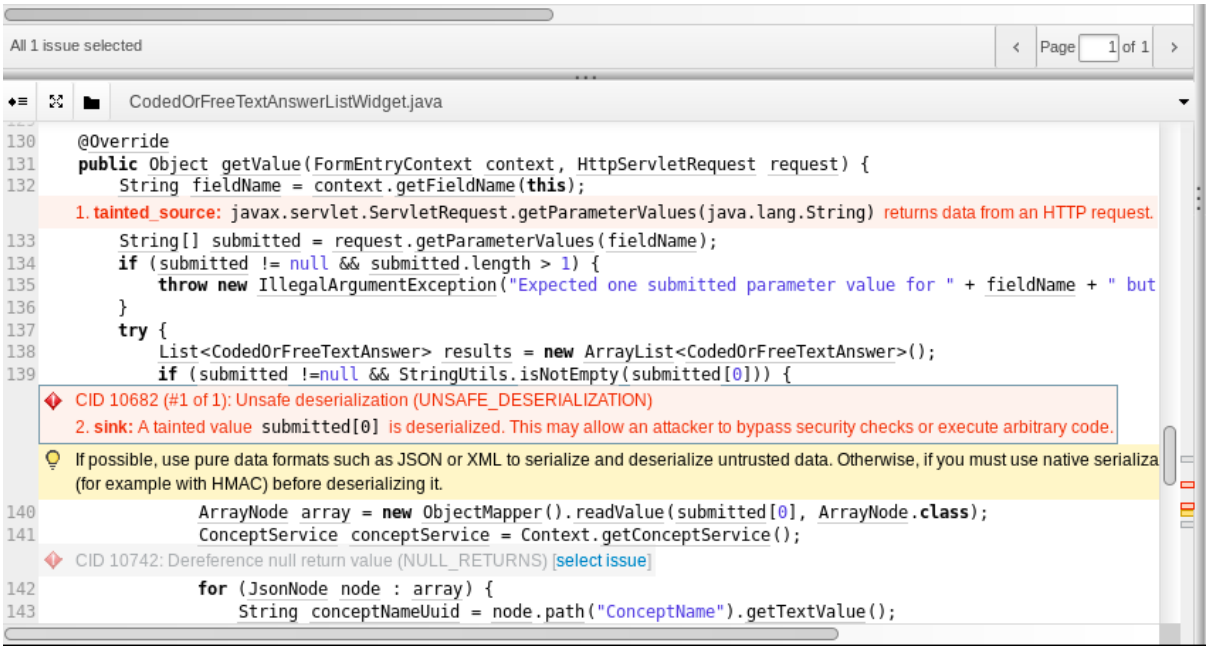
Description:
javax.servlet.ServletRequest.getParameterValues(java.lang.String) returns data from an HTTP request which is stored in a string array-'submitted'.The tainted value submitted[0] is then deserialized. This may allow an attacker to bypass security checks or execute arbitrary code.

Fix:

1.We should use pure data formats such as JSON or XML to serialize and deserialize untrusted data.

2.One could also use native serialization methods to check the integrity of the data (for example with HMAC) before deserializing it.

Snapshot:



6. **Module Name** – coreapps
   CID 12474: Unsafe deserialization
   Category: High Impact Security
   ASVS:5.5.3 –
   Verify that deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).

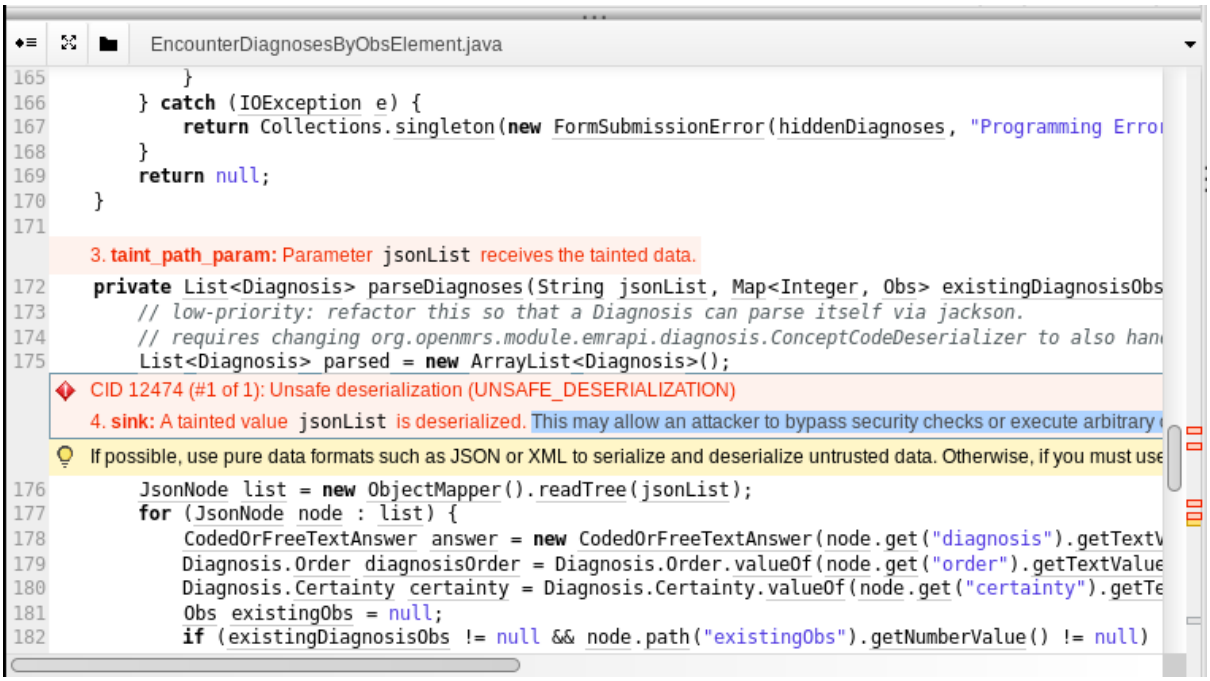
   CWE:502
   Vulnerability type:True Positive

   Description:
   The data from an HTTP request is passed and stored into a string ‘submitted’ which is passed to another string ‘jsonList’ in the code.The tainted value ‘jsonList’ is then deserialize allowing any attacker to bypass security checks or execute arbitrary code.

   Fix:

   Use pure data formats such as JSON or XML to serialize and deserialize untrusted data. Otherwise, if you must use native serialization methods, check the integrity of the data (for example with HMAC) before deserializing it.

   Snapshot:



7. **Module Name** – idgen
   CID 11096: Cross-site request forgery
   Category: High Impact Security
   ASVS:4.2.2 - Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.
   CWE: 352
   Vulnerability type:True Positive

   Description:

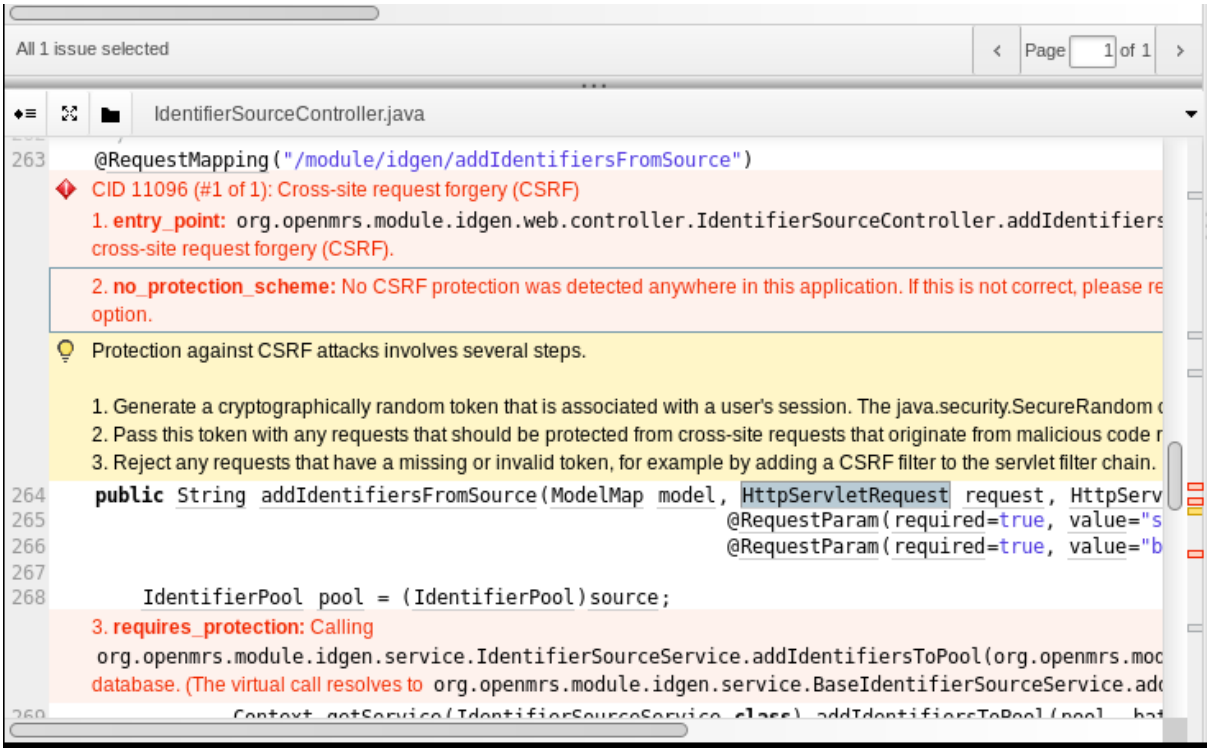
   org.openmrs.module.idgen.web.controller.IdentifierSourceController.addIdentifiersFromSource, the web-app entry point requires protection from cross-site request forgery (CSRF) which is not present.This make the application susceptible to CSRF attack.

Vulnerability Fix:
Protection against CSRF attacks involves several steps.
1. Generate a cryptographically random token that is associated with a user's session. The java.security.SecureRandom class is well suited for this purpose.

2. Pass this token with any requests that should be protected from cross-site requests that originate from malicious code running in a user's browser.

3. Reject any requests that have a missing or invalid token, for example by adding a CSRF filter to the servlet filter chain.

Snapshot:

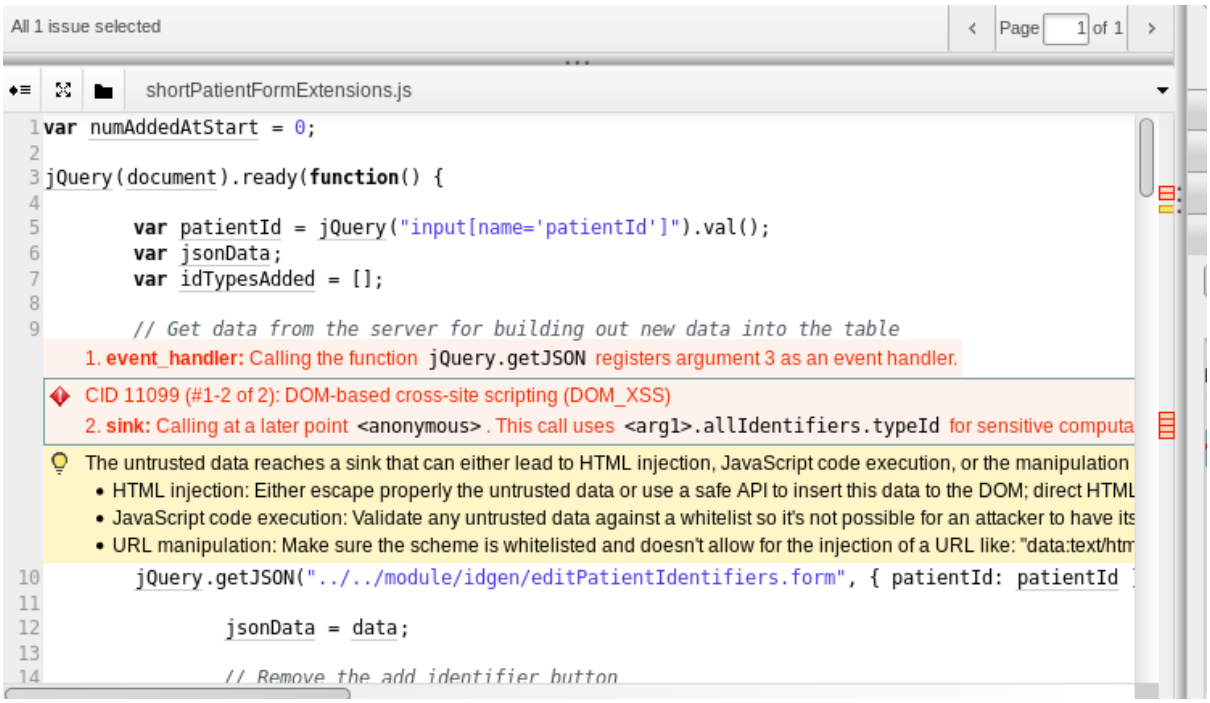


8. **Module Name** – idgen

CID 11099: DOM based cross-site request forgery
Category: High Impact Security
ASVS:5.3.3 - Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.
CWE: 79
Vulnerability type: True Positive
Description:
The application accepts the data provided by the user to the Document Object Model (DOM). This data is then read from the DOM passed to another jQuery.Since the data is not correctly handled, an attacker can inject a payload, which will be stored as part of the DOM and executed when the data is read back from the DOM.

Fix:
1.To prevent DOM XSS one should sanitize all untrusted data, even if it is only used in client-side scripts. When one needs to have user input, always use it in the text context, never as HTML tags or any other potential code.
2.Avoid methods such as document.innerHTML and instead use safer functions,such as, document.innerText and document.textContent.
3.Avoid using user input, especially if it affects DOM elements such as the document.url, the document.location, or the document.referrer.

Snapshot:



9. **Module Name** – idgen
   CID 11120:Unsafe deserialization
   Category: High Impact Security
   ASVS: 5.5.1 - Verify that serialized objects use integrity checks or are encrypted to prevent
   hostile object creation or data tampering.
   CWE: 502
   Vulnerability type:True Positive

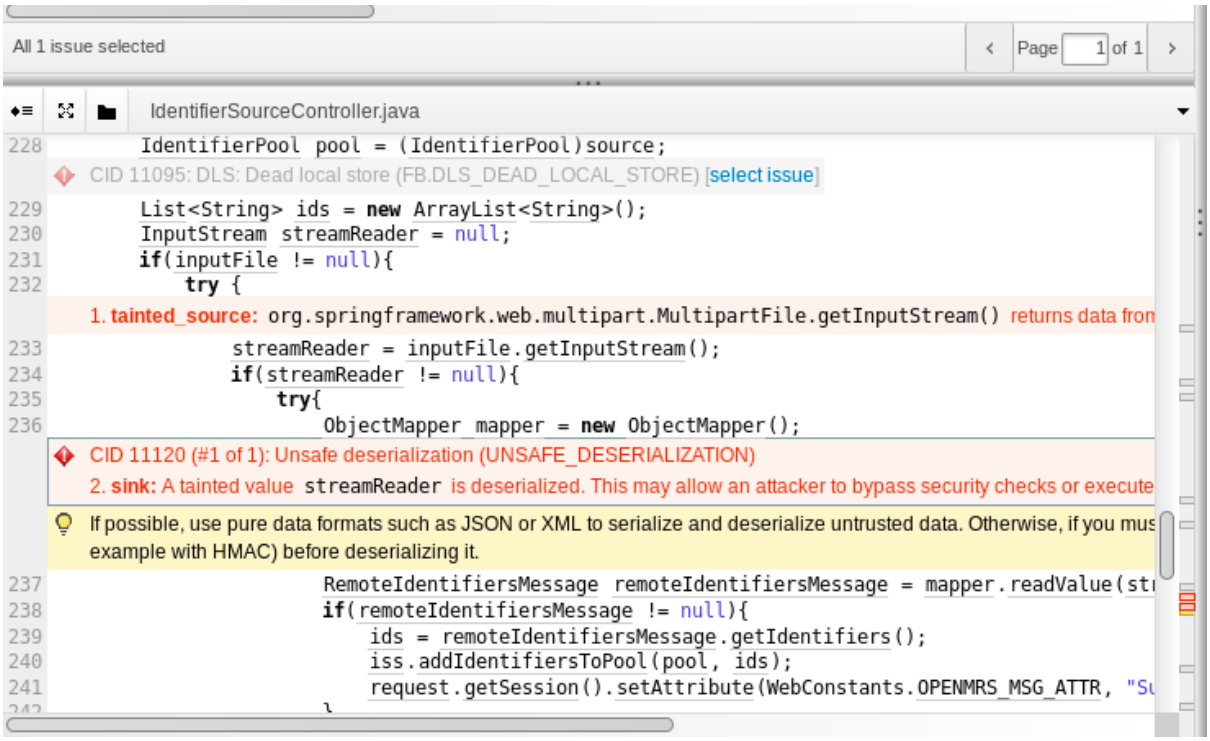
   Description:

   org.springframework.web.multipart.MultipartFile.getInputStream() returns data from an HTTP request. This tainted value is then deserialized in the subsequent lines of code. This may allow an attacker to bypass security checks or execute arbitrary code.

   Fix:

   Use of pure data formats such as JSON or XML to serialize and deserialize untrusted data. or once could use native serialization methods to check the integrity of the data (for example with HMAC) before deserializing it.

   Snapshot:



10. **Module Name** – idgen
    CID 11098: Unsafe reflection
    Category: Low Impact Security
    ASVS 1.4.3:
    Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.
    CWE:470
    Vulnerability type: True Positive

    Description:

    Context.getRequest().getParameter("toDate") returns the data from an HTTP Request.A tainted value toDate is passed to a reflection API. This may allow an attacker to bypass security checks, obtain unauthorized data, or execute arbitrary code. The value is used unsafely in bytecode, which cannot be displayed.

    Fix:

    Validate tainted data against a limited set of static, trusted reflection classes, methods, or fields. Reflecting on one of these known values can protect the application from such attacks.

    Snapshot:

Time based Metric for Coverity:

Number of defects found per hour using Coverity : 2 Defects per hour
Number of true-positives: 6 defects (3 hours approximately)
Total amount of time spent on analyzing fortify report: 6 hours (approximately)

APPENDIX

The following have been attached with this report:

--- The Fortify report that was generated

--- The CSV files that were generated from the coverity analysis

References:

https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf

https://cwe.mitre.org/

Fortify Security Report

Jan 29, 2020

pgupta25

Executive Summary

Issues Overview

On Jan 29, 2020, a source code review was performed over the adminui code base. 902 files, 46,879 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 24 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
High	24

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location:
Number of Files: 902
Lines of Code: 46879
Build Label: <No Build Label>

Scan Information

Scan time: 01:15:52
SCA Engine version: 19.1.0.2241
Machine Name: vclv99-89.hpc.ncsu.edu
Username running scan: pgupta25

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Command Line Arguments:
null.null.null
null.Runner.display_klasses
null.Runner.display_tasks
null.Runner.help
null.Runner.initialize_thorfiles
null.Runner.install
null.Runner.list
null.Runner.method_missing
null.Runner.save_yaml
null.Runner.self.banner
null.Runner.thorfiles
null.Runner.thorfiles_relevant_to
null.Runner.uninstall
null.Runner.update
null.Thor.help
null.Thor.self.banner
null.Thor.self.check_unknown_options!
null.Thor.self.check_unknown_options?
null.Thor.self.create_task

null.Thor.self.default_task
null.Thor.self.desc
null.Thor.self.dispatch
null.Thor.self.find_subcommand
null.Thor.self.find_subcommand_and_update_argv
null.Thor.self.find_subcommand_possibilities
null.Thor.self.help
null.Thor.self.long_desc
null.Thor.self.map
null.Thor.self.method_option
null.Thor.self.method_options
null.Thor.self.normalize_task_name
null.Thor.self.printable_tasks
null.Thor.self.register
null.Thor.self.retrieve_task_name
null.Thor.self.subcommand
null.Thor.self.subcommand_help
null.Thor.self.task_help

Private Information:
null.null.null

System Information:
null.null.null

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
If impact is not in range [2.5, 5.0] Then hide issue
If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

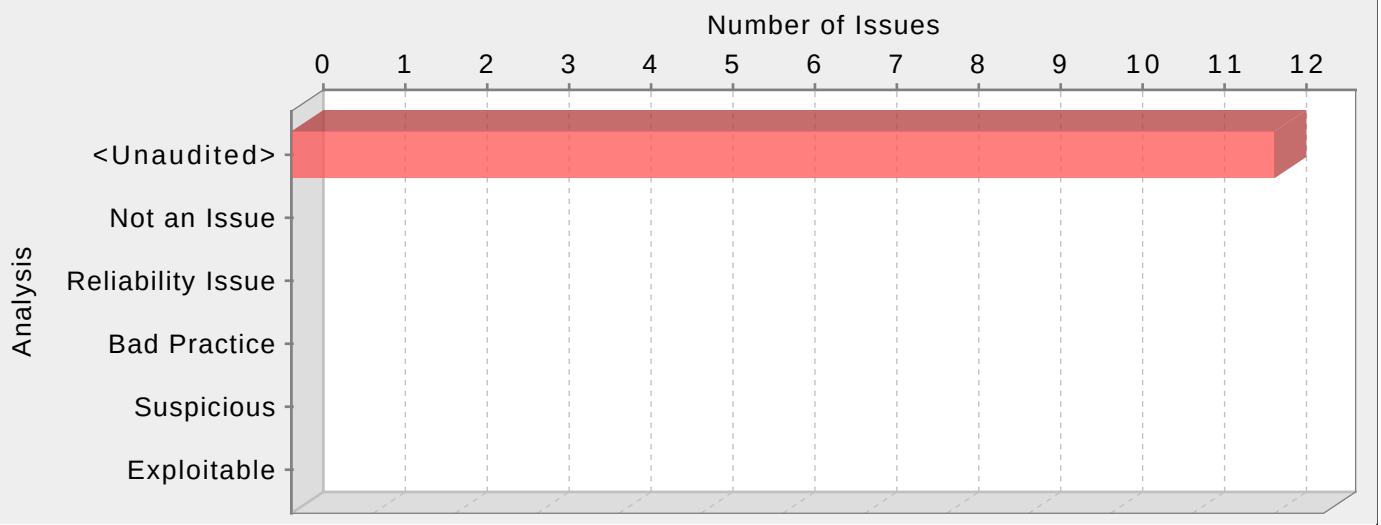
Results Outline

Overall number of results

The scan found 24 issues.

Vulnerability Examples by Category

Category: Password Management: Password in Configuration File (12 Issues)



Abstract:

Storing a plain text password in a configuration file may result in a system compromise.

Explanation:

Storing a plain text password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's job easier. Good password management guidelines require that a password never be stored in plain text.

Recommendations:

A password should never be stored in plain text. An administrator should be required to enter the password when the system starts. If that approach is impractical, a less secure but often adequate solution is to obfuscate the password and scatter the de-obfuscation material around the system so that an attacker has to obtain and correctly combine multiple system resources to decipher the password.

Some third-party products claim the ability to manage passwords in a more secure way. For example, WebSphere Application Server 4.x uses a simple XOR encryption algorithm for obfuscating values, but be skeptical about such facilities. WebSphere and other application servers offer outdated and relatively weak encryption mechanisms that are insufficient for security-sensitive environments. For a secure solution the only viable option is a proprietary one.

Tips:

1. Fortify Static Code Analyzer searches configuration files for common names used for password properties. Audit these issues by verifying that the flagged entry is used as a password and that the password entry contains plain text.

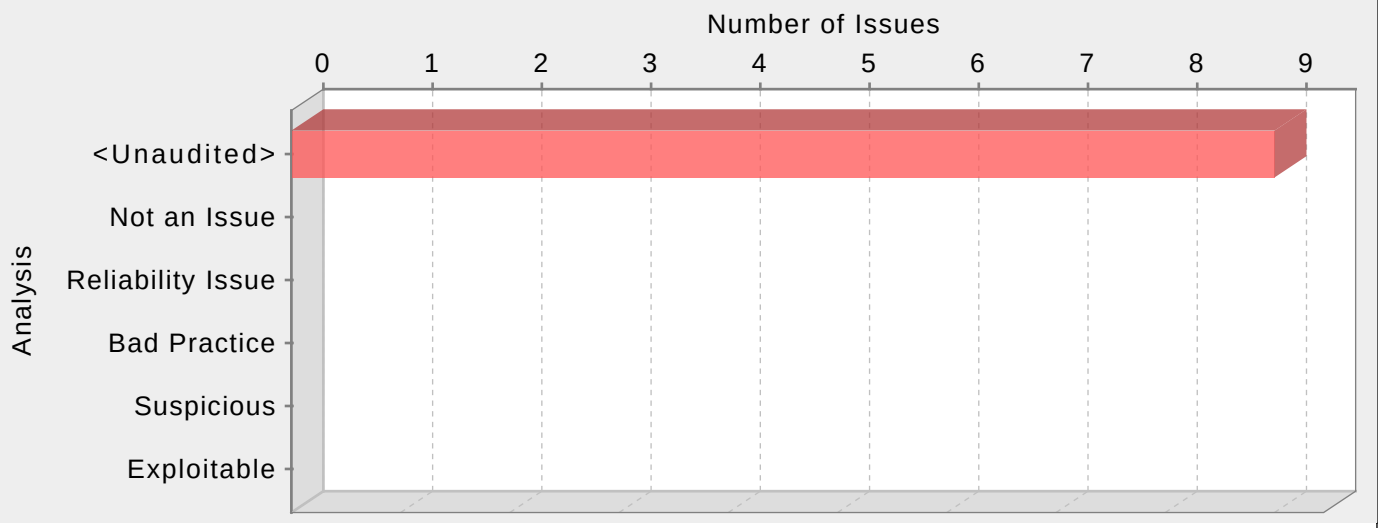
2. If the entry in the configuration file is a default password, require that it be changed in addition to requiring that it be obfuscated in the configuration file.

messages.properties, line 75 (Password Management: Password in Configuration File)

Fortify Priority:	High	**Folder**	High
Kingdom:	Environment		
Abstract:	Storing a plain text password in a configuration file may result in a system compromise.		
Sink:	messages.properties:75 adminui.myAccount.password.label()		

```
73  adminui.myAccount=My Account
74  adminui.myAccount.myLanguages.title=My Languages
75  adminui.myAccount.password.label=Password
76  adminui.myAccount.changeSecretQuestion.label=Secret Question
77  adminui.myAccount.defaults.label=User Defaults
```

Category: Dynamic Code Evaluation: Code Injection (9 Issues)



Abstract:

The file actions.rb interprets unvalidated user input as source code on line 217. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.

Explanation:

Many modern programming languages allow dynamic interpretation of source instructions. This capability allows programmers to perform dynamic instructions based on input received from the user. Code injection vulnerabilities occur when the programmer incorrectly assumes that instructions supplied directly from the user will perform only innocent operations, such as performing simple calculations on active user objects or otherwise modifying the user's state. However, without proper validation, a user might specify operations the programmer does not intend.

Example: In this code injection example, the application implements a basic calculator that allows the user to specify commands for execution.

```
...
user_ops = req['operation']
result = eval(user_ops)
...
```

The program behaves correctly when the operation parameter is a benign value, such as "8 + 7 * 2", in which case the result variable is assigned a value of 22. However, if an attacker specifies languages operations that are both valid and malicious, those operations would be executed with the full privilege of the parent process. Such attacks are even more dangerous when the underlying language provides access to system resources or allows execution of system commands. With Ruby this is allowed, and as multiple commands can be ran by delimiting the lines with a semi-colon (;), it would also enable being able to run many commands with a simple injection, whilst still not breaking the program.

If an attacker were to submit for the parameter operation "system(\"nc -l 4444 &\");8+7*2", then this would open port 4444 to listen for a connection on the machine, and then would still return the value of 22 to result

Recommendations:

Avoid interpreting dynamic code whenever possible. If your program must interpret code dynamically, you can minimize the likelihood of a successful attack by constraining the code that your program will execute dynamically as much as possible, limiting it to a program- and context-specific subset of the base programming language. Unvalidated user input should never be directly interpreted and executed by the program. Instead, use a level of indirection: create a list of legitimate operations and data objects that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never executed directly.

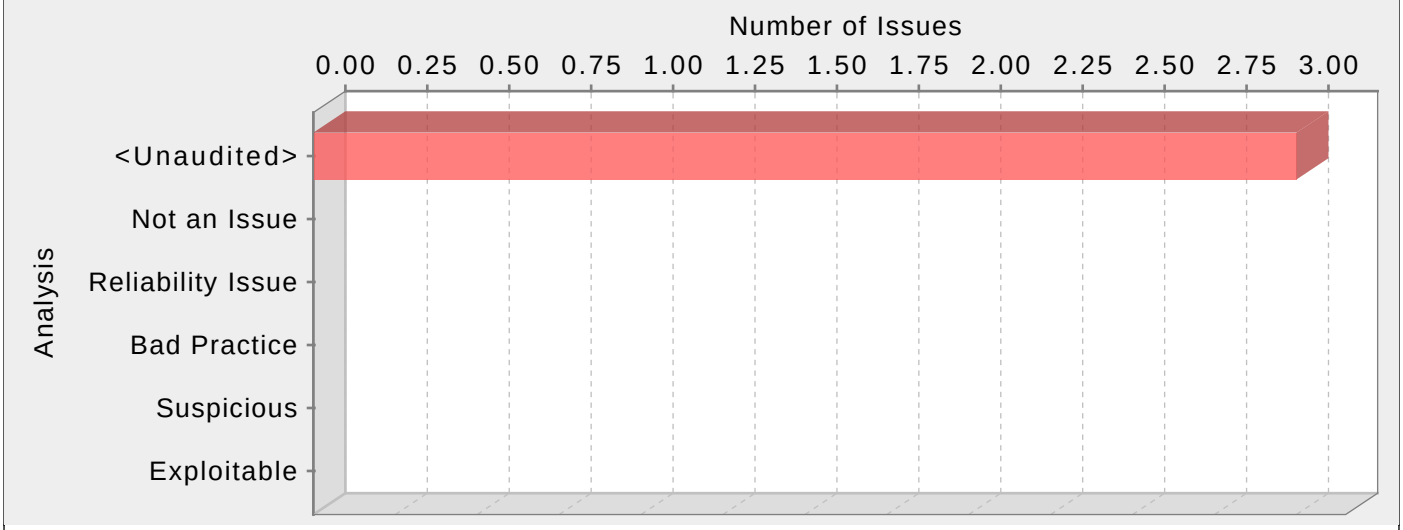
actions.rb, line 217 (Dynamic Code Evaluation: Code Injection)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The file actions.rb interprets unvalidated user input as source code on line 217. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.		

Sink: actions.rb:217 FunctionCall: instance_eval()

```
215         end
216
217         instance_eval(contents, path)
218         shell.padding -= 1 if verbose
219       end
```

Category: Password Management: Hardcoded Password (3 Issues)



Abstract:

Hardcoded passwords may compromise system security in a way that cannot be easily remedied.

Explanation:

It is never a good idea to hardcode a password. Not only does hardcoding a password allow all of the project's developers to view the password, it also makes fixing the problem extremely difficult. After the code is in production, the password cannot be changed without patching the software. If the account protected by the password is compromised, the owners of the system must choose between security and availability.

Example: The following code uses a hardcoded password to connect to an application and retrieve address book entries:

...
obj = new XMLHttpRequest();
obj.open('GET','/fetchusers.jsp?id='+form.id.value,'true','scott','tiger');
...

This code will run successfully, but anyone who accesses the containing web page will be able to view the password.

Recommendations:

Passwords should never be hardcoded and should generally be obfuscated and managed in an external source. Storing passwords in plain text anywhere on the web site allows anyone with sufficient permissions to read and potentially misuse the password. For JavaScript calls that require passwords, it is better to prompt the user for the password at connection time.

Tips:

1. Avoid hardcoding passwords in source code and avoid using default passwords. If a hardcoded password is the default, require that it be changed and remove it from the source code.

2. To identify null, empty, or hardcoded passwords, default rules only consider fields and variables that contain the word password. However, the Fortify Custom Rules Editor provides the Password Management wizard that makes it easy to create rules for detecting password management issues on custom-named fields and variables.

userDetails.js, line 139 (Password Management: Hardcoded Password)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	Hardcoded passwords may compromise system security in a way that cannot be easily remedied.		

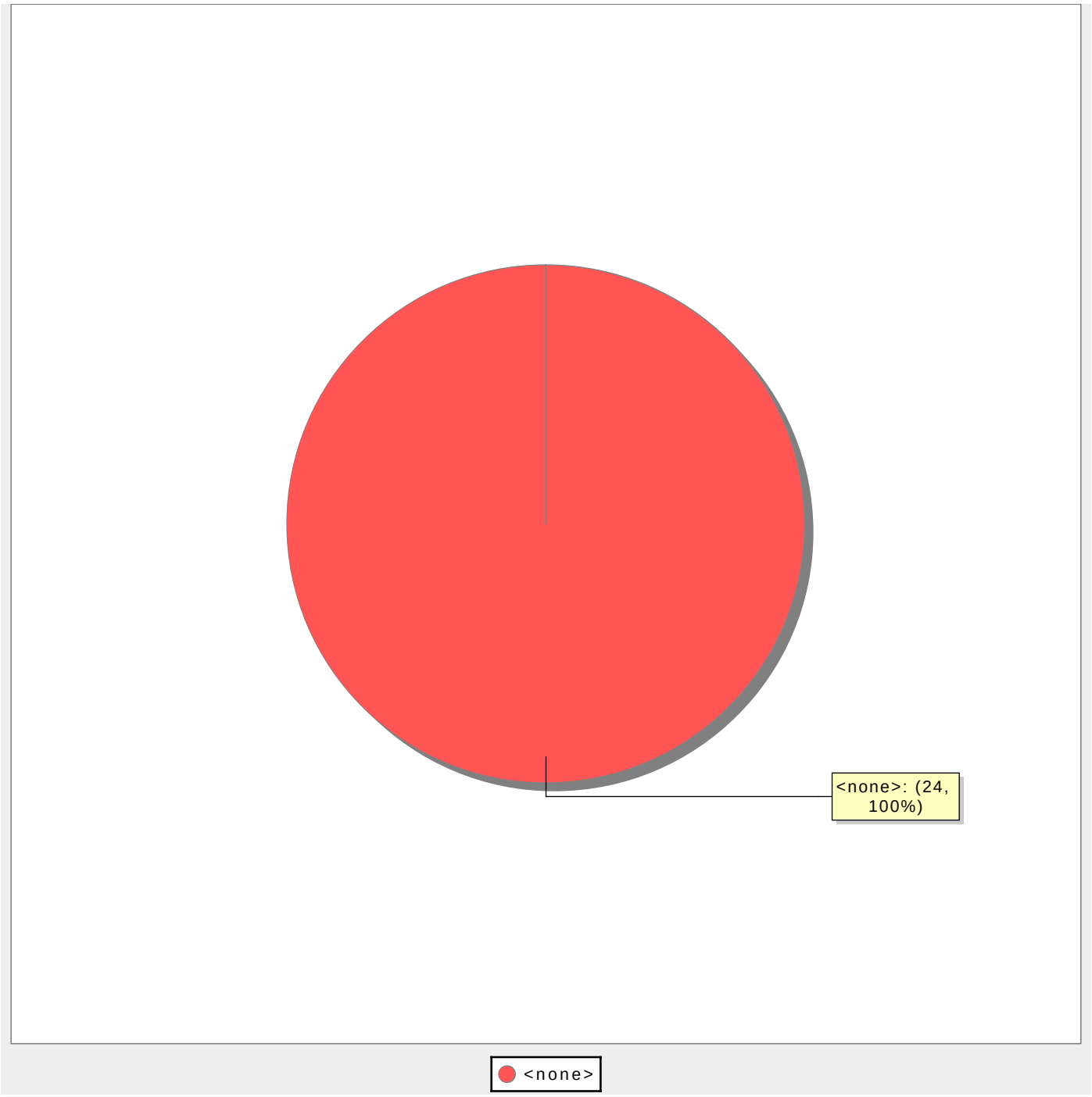
Sink: userDetails.js:139 FieldAccess: forcePassword()

```
137                         var uProperties = {};
138                         if(modelUser.userProperties.forcePassword){
139                             uProperties.forcePassword =******
140                         }
141                         angular.forEach(modelUser.userProperties, function(value, key) {
```

Issue Count by Category	
Issues by Category	
Password Management: Password in Configuration File	12
Dynamic Code Evaluation: Code Injection	9
Password Management: Hardcoded Password	3

Issue Breakdown by Analysis

Issues by Analysis



Fortify Security Report

Jan 23, 2020

pgupta25

Executive Summary

Issues Overview

On Jan 23, 2020, a source code review was performed over the appointmentscheduling code base. 315 files, 31,941 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 114 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
Critical	102
High	12

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: /srv/openmrs_code/org/openmrs/module/appointmentscheduling
Number of Files: 315
Lines of Code: 31941
Build Label: <No Build Label>

Scan Information

Scan time: 29:30
SCA Engine version: 19.1.0.2241
Machine Name: vclv99-89.hpc.ncsu.edu
Username running scan: pgupta25

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Private Information:
null.null.null

System Information:
null.null.null
java.lang.Throwable.getMessage

Web:
javax.servlet.http.HttpServletRequest.getMethod

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High

If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
If impact is not in range [2.5, 5.0] Then hide issue
If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

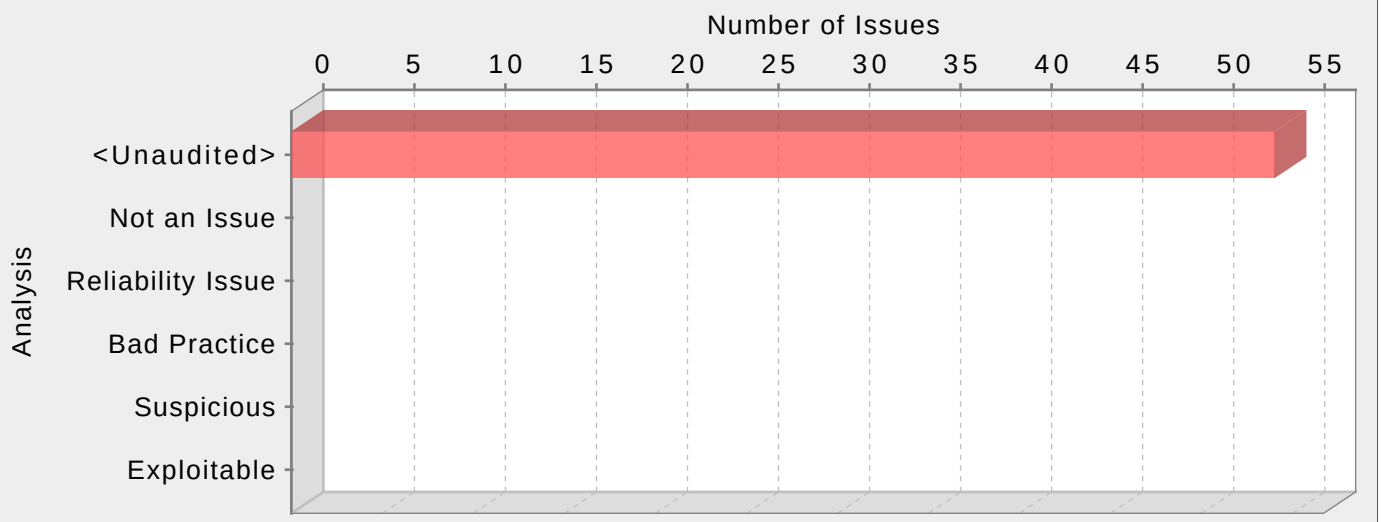
Results Outline

Overall number of results

The scan found 114 issues.

Vulnerability Examples by Category

Category: Cross-Site Scripting: DOM (54 Issues)



Abstract:

The method addNewAppointment() in appointments.jsp sends unvalidated data to a web browser on line 18, which can result in the browser executing malicious code.

Explanation:

Cross-site scripting (XSS) vulnerabilities occur when:

1. Data enters a web application through an untrusted source. In the case of DOM-based XSS, data is read from a URL parameter or other value within the browser and written back into the page with client-side code. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store.

2. The data is included in dynamic content that is sent to a web user without being validated. In the case of DOM Based XSS, malicious content gets executed as part of DOM (Document Object Model) creation, whenever the victim's browser parses the HTML page.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Example 1: The following JavaScript code segment reads an employee ID, eid, from a URL and displays it to the user.

```
<SCRIPT>
var pos=document.URL.indexOf("eid=")+4;
document.write(document.URL.substring(pos,document.URL.length));
</SCRIPT>
```

Example 2: Consider the HTML form:

```
<div id="myDiv">
Employee ID: <input type="text" id="eid"><br>
...
<button>Show results</button>
</div>
<div id="resultsDiv">
...
</div>
```

The following jQuery code segment reads an employee ID from the form, and displays it to the user.

```
$(document).ready(function(){
$("#myDiv").on("click", "button", function(){
var eid = $("#eid").val();
$("resultsDiv").append(eid);
...
});
});
```

These code examples operate correctly if the employee ID, from the text input with ID eid contains only standard alphanumeric text. If eid has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Example 3: The following code shows an example of a DOM-based XSS within a React application:

```
let element = JSON.parse(getUntrustedInput());
ReactDOM.render(<App>
{element}
</App>);
```

In Example 3, if an attacker can control the entire JSON object retrieved from getUntrustedInput(), they may be able to make React render element as a component, and therefore can pass an object with dangerouslySetInnerHTML with their own controlled value, a typical cross-site scripting attack.

Initially these might not appear to be much of a vulnerability. After all, why would someone provide input containing malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS.

As the example demonstrates, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim:

- Data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities.

- The application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

- A source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

Recommendations:

The solution to XSS is to ensure that validation occurs in the correct places and checks are made for the correct properties.

Since XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user.

The most secure approach to validation for XSS is to create a whitelist of safe characters that are allowed to appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alpha-numeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser should still be considered valid input once they are encoded, such as a web design bulletin board that must accept HTML fragments from its users.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines what characters have special meaning, many web browsers try to correct common mistakes in HTML and may treat other characters as special in certain contexts, which is why we do not encourage the use of blacklists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]:

In the content of a block-level element (in the middle of a paragraph of text):

- "<" is special because it introduces a tag.

- "&" is special because it introduces a character entity.

- ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error.

The following principles apply to attribute values:

- In attribute values enclosed with double quotes, the double quotes are special because they mark the end of the attribute value.

- In attribute values enclosed with single quote, the single quotes are special because they mark the end of the attribute value.

- In attribute values without any quotes, white-space characters, such as space and tab, are special.

- "&" is special when used with certain attributes, because it introduces a character entity.

In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters:

- Space, tab, and new line are special because they mark the end of the URL.

- "&" is special because it either introduces a character entity or separates CGI parameters.

- Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context.

- The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server -side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page in question.

Within the body of a <SCRIPT> </SCRIPT>:

- Semicolons, parentheses, curly braces, and new line characters should be filtered out in situations where text could be inserted directly into a pre-existing script tag.

Server-side scripts:

- Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering.

Other possibilities:

- If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and may bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7).

After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option in this situation is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and may be unacceptable in circumstances where the integrity of the input must be preserved for display.

If input containing special characters must be accepted and displayed accurately, validation must encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2].

Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

Tips:

1. The Fortify Secure Coding Rulepacks warn about SQL Injection and Access Control: Database issues when untrusted data is written to a database and also treat the database as a source of untrusted data, which can lead to XSS vulnerabilities. If the database is a trusted resource in your environment, use custom filters to filter out dataflow issues that include the DATABASE taint flag or originate from database sources. Nonetheless, it is often still a good idea to validate everything read from the database.

2. Even though URL encoding untrusted data protects against many XSS attacks, some browsers (specifically, Internet Explorer 6 and 7 and possibly others) automatically decode content at certain locations within the Document Object Model (DOM) prior to passing it to the JavaScript interpreter. To reflect this danger, the rulepacks no longer treat URL encoding routines as sufficient to protect against cross-site scripting. Data values that are URL encoded and subsequently output will cause Fortify to report Cross-Site Scripting: Poor Validation vulnerabilities.

3. Older versions of React are more susceptible to cross-site scripting attacks by controlling an entire component. Newer versions use Symbols to identify a React component, which prevents the exploit, however older browsers that do not have Symbol support (natively, or through polyfills), such as all versions of Internet Explorer, are still vulnerable. Other types of cross-site scripting attacks are valid for all browsers and versions of React.

appointments.jsp, line 18 (Cross-Site Scripting: DOM)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The method addNewAppointment() in appointments.jsp sends unvalidated data to a web browser on line 18, which can result in the browser executing malicious code.		

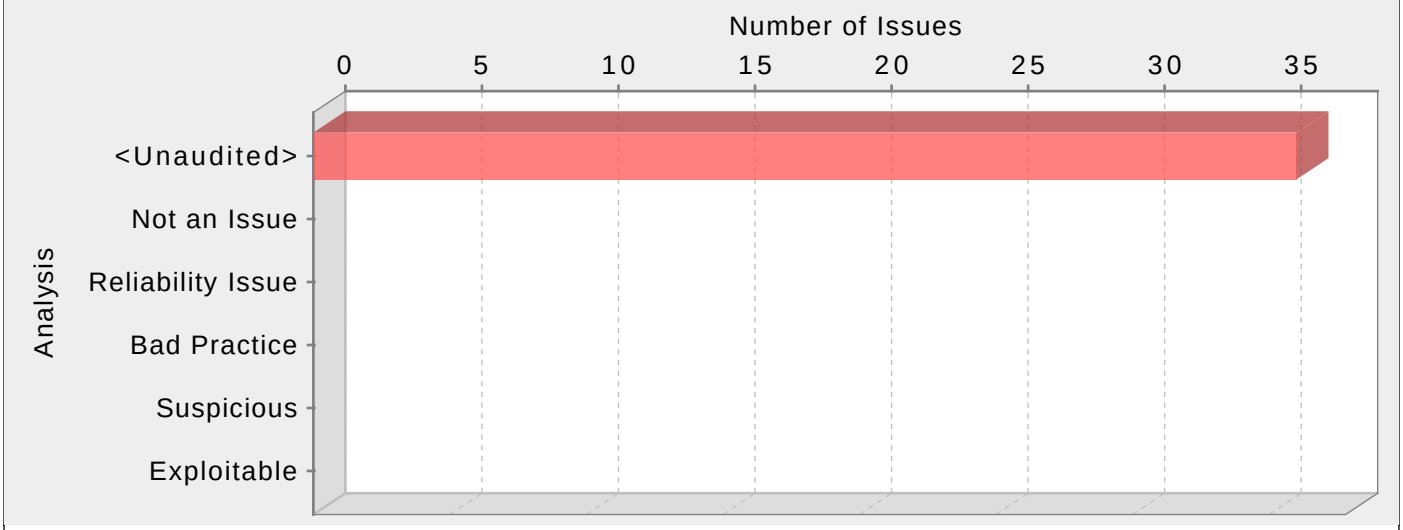
Source: appointments.jsp:17 Read value()

```
15    //Navigate to appointmentForm.form
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
```

Sink: appointments.jsp:18 Assignment to window.location()

```
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
20    //On the page load updates necessary stuff
```

Category: Cross-Site Scripting: Reflected (36 Issues)



Abstract:

The method _jspService() in appointmentForm.jsp sends unvalidated data to a web browser on line 113, which can result in the browser executing malicious code.

Explanation:

Cross-site scripting (XSS) vulnerabilities occur when:

1. Data enters a web application through an untrusted source. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store.

2. The data is included in dynamic content that is sent to a web user without being validated.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Example 1: The following JSP code segment reads an employee ID, eid, from an HTTP request and displays it to the user.

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The code in this example operates correctly if eid contains only standard alphanumeric text. If eid has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL which causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS.

Example 2: The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

```
<%...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
}
%>
Employee Name: <%= name %>
```

As in Example 1, this code functions correctly when the values of name are well-behaved, but it does nothing to prevent exploits if they are not. Again, this code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker may execute malicious commands in the user's web browser. This type of exploit, known as Persistent (or Stored) XSS, is particularly insidious because the indirection caused by the data store makes it more difficult to identify the threat and increases the possibility that the attack will affect multiple users. XSS got its start in this form with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code.

Some think that in the mobile world, classic web application vulnerabilities, such as cross-site scripting, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 3: The following code enables JavaScript in Android's WebView (by default, JavaScript is disabled) and loads a page based on the value received from an Android intent.

```
...
WebView webview = (WebView) findViewById(R.id.webview);
webview.getSettings().setJavaScriptEnabled(true);
String url = this.getIntent().getExtras().getString("url");
webview.loadUrl(url);
...
```

If the value of url starts with javascript:, JavaScript code that follows will execute within the context of the web page inside WebView.

As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim:

- As in Example 1, data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities.

- As in Example 2, the application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

- As in Example 3, a source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, the rulepacks dynamically re-prioritize the issues reported by Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

Recommendations:

The solution to XSS is to ensure that validation occurs in the correct places and checks are made for the correct properties.

Since XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user.

The most secure approach to validation for XSS is to create a whitelist of safe characters that are allowed to appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alpha-numeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser should still be considered valid input once they are encoded, such as a web design bulletin board that must accept HTML fragments from its users.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines what characters have special meaning, many web browsers try to correct common mistakes in HTML and may treat other characters as special in certain contexts, which is why we do not encourage the use of blacklists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]:

In the content of a block-level element (in the middle of a paragraph of text):

- "<" is special because it introduces a tag.

- "&" is special because it introduces a character entity.

- ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error.

The following principles apply to attribute values:

- In attribute values enclosed with double quotes, the double quotes are special because they mark the end of the attribute value.

- In attribute values enclosed with single quote, the single quotes are special because they mark the end of the attribute value.

- In attribute values without any quotes, white-space characters, such as space and tab, are special.

- "&" is special when used with certain attributes, because it introduces a character entity.

In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters:

- Space, tab, and new line are special because they mark the end of the URL.

- "&" is special because it either introduces a character entity or separates CGI parameters.

- Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context.

- The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server -side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page in question.

Within the body of a <SCRIPT> </SCRIPT>:

- Semicolons, parentheses, curly braces, and new line characters should be filtered out in situations where text could be inserted directly into a pre-existing script tag.

Server-side scripts:

- Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering.

Other possibilities:

- If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and may bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7).

After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option in this situation is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and may be unacceptable in circumstances where the integrity of the input must be preserved for display.

If input containing special characters must be accepted and displayed accurately, validation must encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2].

Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

Tips:

1. The Fortify Secure Coding Rulepacks warn about SQL Injection and Access Control: Database issues when untrusted data is written to a database and also treat the database as a source of untrusted data, which can lead to XSS vulnerabilities. If the database is a trusted resource in your environment, use custom filters to filter out dataflow issues that include the DATABASE taint flag or originate from database sources. Nonetheless, it is often still a good idea to validate everything read from the database.

2. Even though URL encoding untrusted data protects against many XSS attacks, some browsers (specifically, Internet Explorer 6 and 7 and possibly others) automatically decode content at certain locations within the Document Object Model (DOM) prior to passing it to the JavaScript interpreter. To reflect this danger, the rulepacks no longer treat URL encoding routines as sufficient to protect against cross-site scripting. Data values that are URL encoded and subsequently output will cause Fortify to report Cross-Site Scripting: Poor Validation vulnerabilities.

3. Fortify RTA adds protection against this category.

appointmentForm.jsp, line 113 (Cross-Site Scripting: Reflected)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The method _jspService() in appointmentForm.jsp sends unvalidated data to a web browser on line 113, which can result in the browser executing malicious code.		

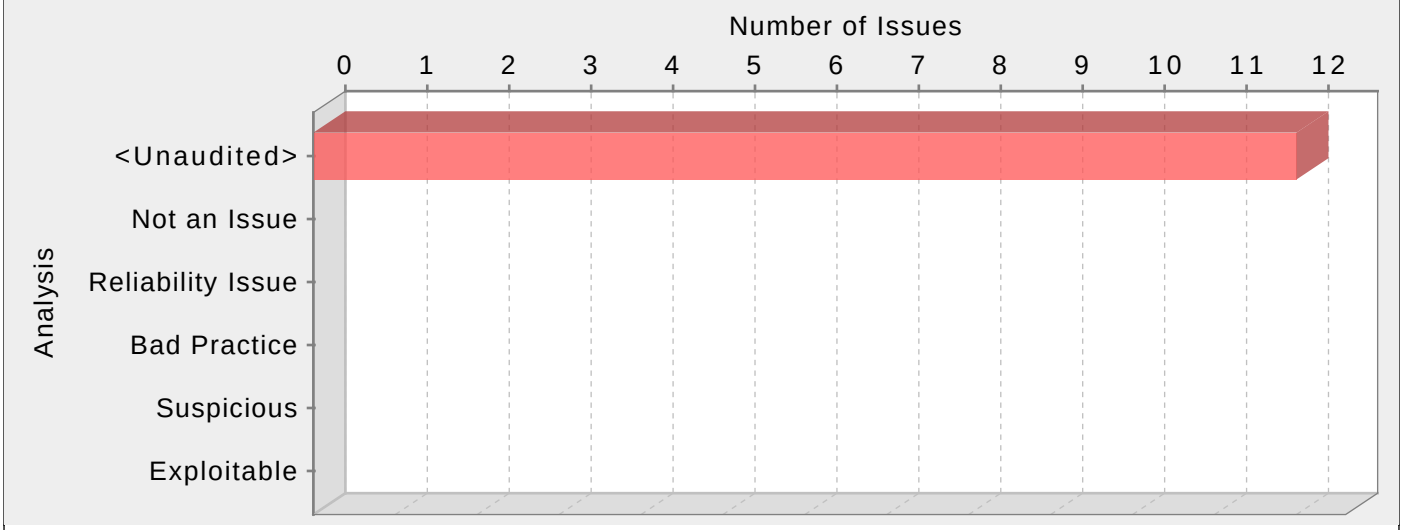
Source: appointmentForm.jsp:113 javax.servlet.ServletRequest.getParameter()

```
111                         "<input type=\"checkbox\" name=\"includeFull\" value=\"true\"
onchange='this.form.submit();' ${(param.includeFull=='true') ? 'checked' : ''}>"+
112                          "<spring:message code='appointmentscheduling.Appointment.create.label.showFu
113                          "<br/><c:if test='${param.includeFull==\'true\'}'>"+
114                          "<div id='slotIndex'> <img
src='${pageContext.request.contextPath}/moduleResources/appointmentscheduling/Images/i
ndex_fullTimeslot.png' alt='<spring:message
code='appointmentscheduling.Appointment.create.lbl.fullSlot'/>'/>"+
115                          " = <spring:message
code='appointmentscheduling.Appointment.create.lbl.fullSlot'/></div></c:if>"+
```

Sink: appointmentForm.jsp:113 javax.servlet.jsp.JspWriter.print()

```
111                         "<input type=\"checkbox\" name=\"includeFull\" value=\"true\"
onchange='this.form.submit();' ${(param.includeFull=='true') ? 'checked' : ''}>"+
112                          "<spring:message code='appointmentscheduling.Appointment.create.label.showFu
113                          "<br/><c:if test='${param.includeFull==\'true\'}'>"+
114                          "<div id='slotIndex'> <img
src='${pageContext.request.contextPath}/moduleResources/appointmentscheduling/Images/i
ndex_fullTimeslot.png' alt='<spring:message
code='appointmentscheduling.Appointment.create.lbl.fullSlot'/>'/>"+
115                          " = <spring:message
code='appointmentscheduling.Appointment.create.lbl.fullSlot'/></div></c:if>"+
```

Category: Header Manipulation: Cookies (12 Issues)



Abstract:

The method _fnCreateCookie() in jquery.dataTables.js includes unvalidated data in an HTTP cookie on line 4554. This enables Cookie manipulation attacks and can lead to other HTTP Response header manipulation attacks like: cache-poisoning, cross-site scripting, cross-user defacement, page hijacking or open redirect.

Explanation:

Cookie Manipulation vulnerabilities occur when:

1. Data enters a web application through an untrusted source, most frequently an HTTP request.

2. The data is included in an HTTP cookie sent to a web user without being validated.

As with many software security vulnerabilities, cookie manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP cookie.

Cookie Manipulation: When combined with attacks like cross-site request forgery, attackers may change, add to, or even overwrite a legitimate user's cookies.

Being an HTTP Response header, Cookie manipulation attacks can also lead to other types of attacks like:

HTTP Response Splitting:

One of the most common Header Manipulation attacks is HTTP Response Splitting. To mount a successful HTTP Response Splitting exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header. These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allows them to create additional responses entirely under their control.

Many of today's modern application servers will prevent the injection of malicious characters into HTTP headers. For example, recent versions of Apache Tomcat will throw an IllegalArgumentException if you attempt to set a header with prohibited characters. If your application server prevents setting headers with new line characters, then your application is not vulnerable to HTTP Response Splitting. However, solely filtering for new line characters can leave an application vulnerable to Cookie Manipulation or Open Redirects, so care must still be taken when setting HTTP headers with user input.

Example: The following code segment reads the name of the author of a weblog entry, author, from an HTTP request and sets it in a cookie header of an HTTP response.

```
author = form.author.value;
...
document.cookie = "author=" + author + ";expires="+cookieExpiration;
...
```

Assuming a string consisting of standard alpha-numeric characters, such as "Jane Smith", is submitted in the request the HTTP response including this cookie might take the following form:

```
HTTP/1.1 200 OK
...
Set-Cookie: author=Jane Smith
...
```

However, because the value of the cookie is formed of unvalidated user input the response will only maintain this form if the value submitted for AUTHOR_PARAM does not contain any CR and LF characters. If an attacker submits a malicious string, such as "Wiley Hacker\r\nHTTP/1.1 200 OK\r\n...", then the HTTP response would be split into two responses of the following form:

HTTP/1.1 200 OK

...
Set-Cookie: author=Wiley Hacker

HTTP/1.1 200 OK

...

Clearly, the second response is completely controlled by the attacker and can be constructed with any header and body content desired. The ability of attacker to construct arbitrary HTTP responses permits a variety of resulting attacks, including: cross-user defacement, web and browser cache poisoning, cross-site scripting, and page hijacking.

Cross-User Defacement: An attacker will be able to make a single request to a vulnerable server that will cause the server to create two responses, the second of which may be misinterpreted as a response to a different request, possibly one made by another user sharing the same TCP connection with the server. This can be accomplished by convincing the user to submit the malicious request themselves, or remotely in situations where the attacker and the user share a common TCP connection to the server, such as a shared proxy server. In the best case, an attacker may leverage this ability to convince users that the application has been hacked, causing users to lose confidence in the security of the application. In the worst case, an attacker may provide specially crafted content designed to mimic the behavior of the application but redirect private information, such as account numbers and passwords, back to the attacker.

Cache Poisoning: The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a response is cached in a shared web cache, such as those commonly found in proxy servers, then all users of that cache will continue receive the malicious content until the cache entry is purged. Similarly, if the response is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is purged, although only the user of the local browser instance will be affected.

Cross-Site Scripting: Once attackers have control of the responses sent by an application, they have a choice of a variety of malicious content to provide users. Cross-site scripting is common form of attack where malicious JavaScript or other code included in a response is executed in the user's browser. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. The most common and dangerous attack vector against users of a vulnerable application uses JavaScript to transmit session and authentication information back to the attacker who can then take complete control of the victim's account.

Page Hijacking: In addition to using a vulnerable application to send malicious content to a user, the same root vulnerability can also be leveraged to redirect sensitive content generated by the server and intended for the user to the attacker instead. By submitting a request that results in two responses, the intended response from the server and the response generated by the attacker, an attacker may cause an intermediate node, such as a shared proxy server, to misdirect a response generated by the server for the user to the attacker. Because the request made by the attacker generates two responses, the first is interpreted as a response to the attacker's request, while the second remains in limbo. When the user makes a legitimate request through the same TCP connection, the attacker's request is already waiting and is interpreted as a response to the victim's request. The attacker then sends a second request to the server, to which the proxy server responds with the server generated request intended for the victim, thereby compromising any sensitive information in the headers or body of the response intended for the victim.

Open Redirect: Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Recommendations:

The solution to cookie manipulation is to ensure that input validation occurs in the correct places and checks for the correct properties.

Since Header Manipulation vulnerabilities like cookie manipulation occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating responses dynamically, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for Header Manipulation.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for Header Manipulation is generally relatively easy. Despite its value, input validation for Header Manipulation does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent Header Manipulation vulnerabilities is to validate everything that enters the application or leaves the application destined for the user.

The most secure approach to validation for Header Manipulation is to create a whitelist of safe characters that are allowed to appear in HTTP response headers and accept input composed exclusively of characters in the approved set. For example, a valid name might only include alpha-numeric characters or an account number might only include digits 0-9.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning in HTTP response headers. Although the CR and LF characters are at the heart of an HTTP response splitting attack, other characters, such as ':' (colon) and '=' (equal), have special meaning in response headers as well.

After you identify the correct points in an application to perform validation for Header Manipulation attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. The application should reject any input destined to be included in HTTP response headers that contains special characters, particularly CR and LF, as invalid.

Many application servers attempt to limit an application's exposure to HTTP response splitting vulnerabilities by providing implementations for the functions responsible for setting HTTP headers and cookies that perform validation for the characters essential to an HTTP response splitting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

jquery.dataTables.js, line 4554 (Header Manipulation: Cookies)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method _fnCreateCookie() in jquery.dataTables.js includes unvalidated data in an HTTP cookie on line 4554. This enables Cookie manipulation attacks and can lead to other HTTP Response header manipulation attacks like: cache-poisoning, cross-site scripting, cross-user defacement, page hijacking or open redirect.		

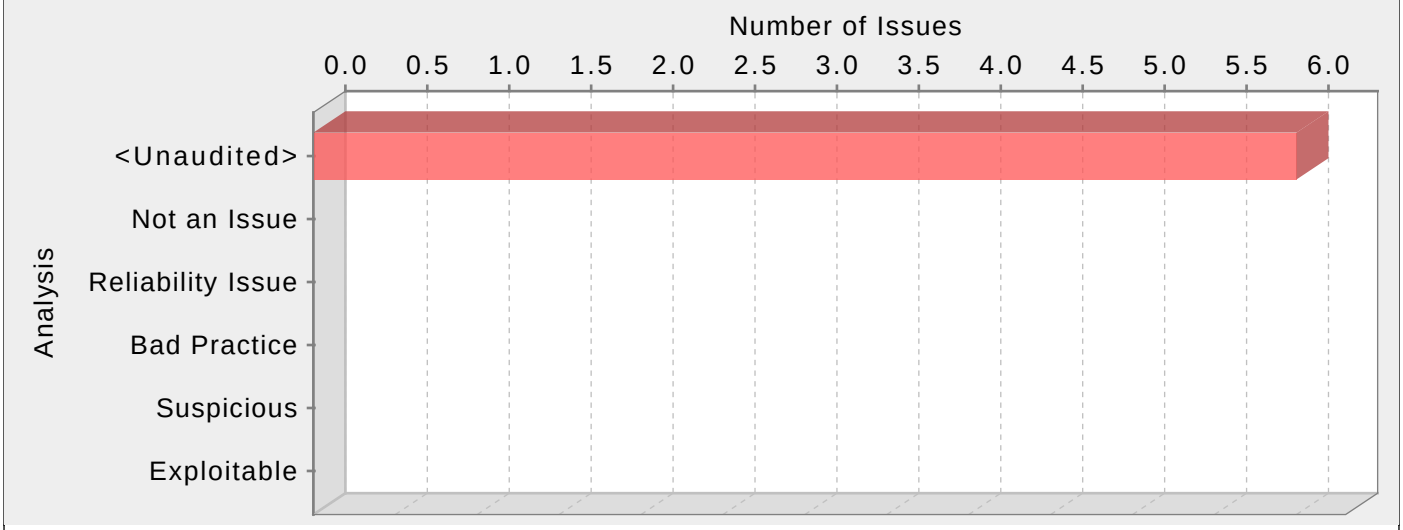
Source: jquery.dataTables.js:4493 Read window.location()

```
4491      * patch to use at least some of the path
4492      */
4493     var aParts = window.location.pathname.split('/');
4494     var sNameFile = sName + '_' + aParts.pop().replace(/[\/:]/g,"").toLowerCase();
4495     var sFullCookie, oData;
```

Sink: jquery.dataTables.js:4554 Assignment to document.cookie()

```
4552
4553       var old = aOldCookies.pop();
4554       document.cookie = old.name+"=; expires=Thu, 01-Jan-1970 00:00:01 GMT; path="+
4555        aParts.join('/') + "/";
4556      }
```

Category: Dynamic Code Evaluation: Code Injection (6 Issues)



Abstract:

The file jquery.dataTables.js interprets unvalidated user input as source code on line 4527. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.

Explanation:

Many modern programming languages allow dynamic interpretation of source instructions. This capability allows programmers to perform dynamic instructions based on input received from the user. Code injection vulnerabilities occur when the programmer incorrectly assumes that instructions supplied directly from the user will perform only innocent operations, such as performing simple calculations on active user objects or otherwise modifying the user's state. However, without proper validation, a user might specify operations the programmer does not intend.

Example: In this classic code injection example, the application implements a basic calculator that allows the user to specify commands for execution.

...
userOp = form.operation.value;
calcResult = eval(userOp);
...

The program behaves correctly when the operation parameter is a benign value, such as "8 + 7 * 2", in which case the calcResult variable is assigned a value of 22. However, if an attacker specifies languages operations that are both valid and malicious, those operations would be executed with the full privilege of the parent process. Such attacks are even more dangerous when the underlying language provides access to system resources or allows execution of system commands. In the case of JavaScript, the attacker may utilize this vulnerability to perform a cross-site scripting attack.

Recommendations:

Avoid dynamic code interpretation whenever possible. If your program's functionality requires code to be interpreted dynamically, the likelihood of attack can be minimized by constraining the code your program will execute dynamically as much as possible, limiting it to an application- and context-specific subset of the base programming language.

If dynamic code execution is required, unvalidated user input should never be directly executed and interpreted by the application. Instead, use a level of indirection: create a list of legitimate operations and data objects that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never executed directly.

jquery.dataTables.js, line 4527 (Dynamic Code Evaluation: Code Injection)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file jquery.dataTables.js interprets unvalidated user input as source code on line 4527. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.		

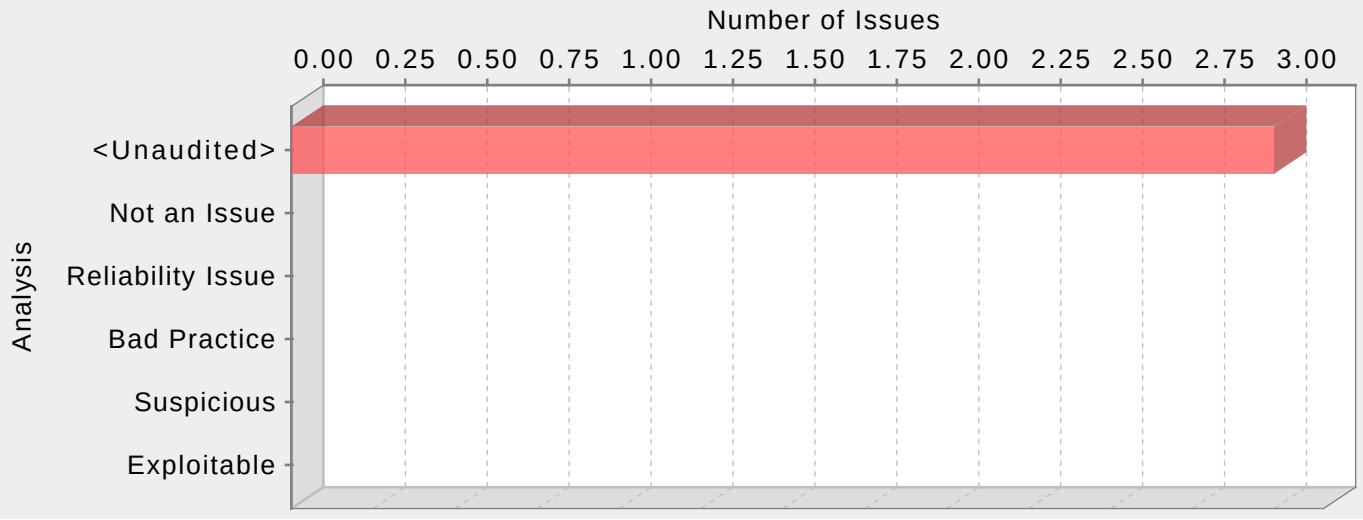
Source: jquery.dataTables.js:4514 Read document.cookie()

```
4512        */
4513       var
4514        aCookies =document.cookie.split(';'),
4515        iNewCookieLen = sFullCookie.split(';')[0].length,
4516        aOldCookies = [];
```

Sink: jquery.dataTables.js:4527 eval()

```
4525                        var aSplitCookie = aCookies[i].split('=');
4526                        try {
4527                         oData = eval( '('+decodeURIComponent(aSplitCookie[1])+')' );
4528
4529                         if ( oData && oData.iCreate )
```

Category: Key Management: Hardcoded Encryption Key (3 Issues)



Abstract:

Hardcoded encryption keys can compromise security in a way that cannot be easily remedied.

Explanation:

It is never a good idea to hardcode an encryption key because it allows all of the project's developers to view the encryption key, and makes fixing the problem extremely difficult. After the code is in production, a software patch is required to change the encryption key. If the account that is protected by the encryption key is compromised, the owners of the system must choose between security and availability.

Example 1: The following code uses a hardcoded encryption key:

```
...
var crypto = require('crypto');
var encryptionKey = "lakdsljkalkjlksdfkl";
var algorithm = 'aes-256-ctr';
var cipher = crypto.createCipher(algorithm, encryptionKey);
...
```

Anyone with access to the code has access to the encryption key. After the application has shipped, there is no way to change the encryption key unless the program is patched. An employee with access to this information can use it to break into the system. If attackers had access to the executable for the application, they could extract the encryption key value.

Recommendations:

Encryption keys should never be hardcoded and should be obfuscated and managed in an external source. Storing encryption keys in plain text anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the encryption key.

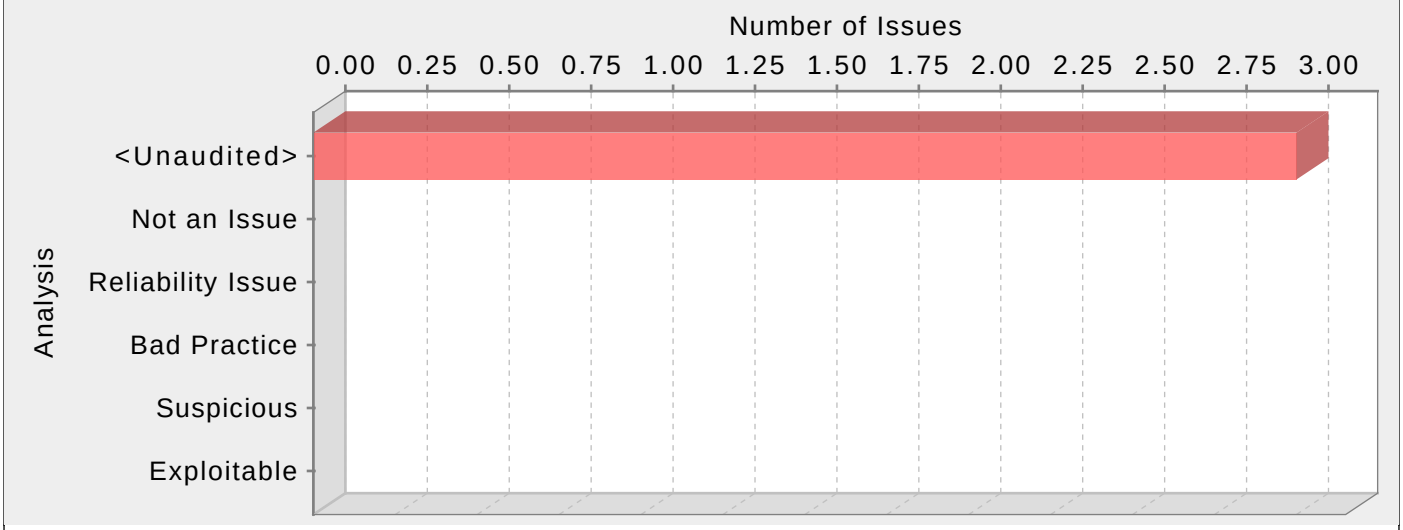
jquery.jeditable.js, line 515 (Key Management: Hardcoded Encryption Key)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Security Features		
Abstract:	Hardcoded encryption keys can compromise security in a way that cannot be easily remedied.		

Sink: jquery.jeditable.js:515 Operation()

```
513                         continue;
514                     }
515                     if ('selected' == key) {
516                         continue;
517                     }
```

Category: Open Redirect (3 Issues)



Abstract:

The file appointments.jsp passes unvalidated data to an HTTP redirect function on line 18. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Explanation:

Redirects allow web applications to direct users to different pages within the same application or to external sites. Applications utilize redirects to aid in site navigation and, in some cases, to track how users exit the site. Open redirect vulnerabilities occur when a web application redirects clients to any arbitrary URL that can be controlled by an attacker.

Attackers may utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. By encoding the URL, an attacker is able to make it more difficult for end-users to notice the malicious destination of the redirect, even when it is passed as a URL parameter to the trusted site. Open redirects are often abused as part of phishing scams to harvest sensitive end-user data.

Example 1: The following JavaScript code instructs the user's browser to open a URL read from the dest request parameter when a user clicks the link.

```
...
strDest = form.dest.value;
window.open(strDest,"myresults");
...
```

If a victim received an email instructing them to follow a link to "http://trusted.example.com/ecommerce/redirect.asp?dest=www.wilyhacker.com", the user would likely click on the link believing they would be transferred to the trusted site. However, when the victim clicks the link, the code in Example 1 will redirect the browser to "http://www.wilyhacker.com".

Many users have been educated to always inspect URLs they receive in emails to make sure the link specifies a trusted site they know. However, if the attacker Hex encoded the destination url as follows:

"http://trusted.example.com/ecommerce/redirect.asp?dest=%77%69%6C%79%68%61%63%6B%65%72%2E%63%6F%6D"

then even a savvy end-user may be fooled into following the link.

Recommendations:

Unvalidated user input should not be allowed to control the destination URL in a redirect. Instead, use a level of indirection: create a list of legitimate URLs that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a URL for redirects.

Example 2: The following code references an array populated with valid URLs. The link the user clicks passes in the array index that corresponds to the desired URL.

```
...
strDest = form.dest.value;
if((strDest.value != null)||(strDest.value.length!=0))
{
if((strDest >= 0) && (strDest <= strURLArray.length -1 ))
{
strFinalURL = strURLArray[strDest];
window.open(strFinalURL,"myresults");
```

```
}
}
...
```

In some situations this approach is impractical because the set of legitimate URLs is too large or too hard to keep track of. In such cases, use a similar approach to restrict the domains that users can be redirected to, which can at least prevent attackers from sending users to malicious external sites.

appointments.jsp, line 18 (Open Redirect)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file appointments.jsp passes unvalidated data to an HTTP redirect function on line 18. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.		

Source: appointments.jsp:17 Read value()

```
15    //Navigate to appointmentForm.form
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
```

Sink: appointments.jsp:18 Assignment to window.location()

```
16    function addNewAppointment(){
17     var patientId = document.getElementById("patientId").value;
18     window.location =
"module/appointmentscheduling/appointmentForm.form?patientId="+patientId;
19    }
20    //On the page load updates necessary stuff
```

Detailed Project Summary

Files Scanned

Code base location: /srv/openmrs_code/org/openmrs/module/appointmentscheduling
Files Scanned:
.travis.yml yaml Dec 13, 2019 12:56:58 PM
OpenMRSFormatter.xml xml 27.9 KB Dec 13, 2019 12:56:58 PM
api/pom.xml xml 1.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/Appointment.java java 56 Lines 5.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentActivator.java java 8 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentBlock.java java 24 Lines 2.6 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentRequest.java java 27 Lines 3.3 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentSchedulingConstants.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentStatusHistory.java java 19 Lines 2.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentType.java java 16 Lines 2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentUtils.java java 18 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/StudentT.java java 122 Lines 9.8 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/TimeFrameUnits.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/TimeSlot.java java 18 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/AppointmentService.java java 36.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/AppointmentBlockDAO.java java 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/AppointmentDAO.java java 3.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/AppointmentRequestDAO.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/AppointmentStatusHistoryDAO.java java 2.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/AppointmentTypeDAO.java java 1.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/SingleClassDAO.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/TimeSlotDAO.java java 2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateAppointmentBlockDAO.java java 27 Lines 6.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateAppointmentDAO.java java 61 Lines 8.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateAppointmentRequestDAO.java java 3 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateAppointmentStatusHistoryDAO.java java 17 Lines 3.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateAppointmentTypeDAO.java java 10 Lines 2.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateSingleClassDAO.java java 18 Lines 3.9

KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/db/hibernate/HibernateTimeSlotDAO.java java 15 Lines 2.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/api/impl/AppointmentServiceImpl.java java 331 Lines 38.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/exception/TimeSlotFullException.java java 3 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/context/AppointmentEvaluationContext.java java 12 Lines 2.6 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/AppointmentData.java java 1 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/AppointmentDataUtil.java java 16 Lines 2.6 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/EvaluatedAppointmentData.java java 8 Lines 1.5 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentCancelReasonDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentDataDefinition.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentEndDateDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentLocationDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentProviderDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentReasonDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentStartDateDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentStatusDataDefinition.java java 4 Lines 1.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/AppointmentTypeDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/PatientToAppointmentDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/definition/PersonToAppointmentDataDefinition.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentCancelReasonDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentDataEvaluator.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentEndDateDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentLocationDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentPropertyDataEvaluator.java java 8 Lines 1.8 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentProviderDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentReasonDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM

api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentStartDateDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentStatusDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentTypeDataEvaluator.java java 2 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/PatientToAppointmentDataEvaluator.java java 21 Lines 4.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/PersonToAppointmentDataEvaluator.java java 22 Lines 4.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/service/AppointmentDataService.java java 1.5 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/data/service/AppointmentDataServiceImpl.java java 6 Lines 2.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/dataset/definition/AppointmentDataSetDefinition.java java 20 Lines 5.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/dataset/evaluator/AppointmentDataSetEvaluator.java java 25 Lines 5.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/AppointmentIdSet.java java 5 Lines Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/AppointmentQueryResult.java java 8 Lines 1.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/definition/AppointmentQuery.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/definition/BasicAppointmentQuery.java java 8 Lines 2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/evaluator/AppointmentQueryEvaluator.java java Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/evaluator/BasicAppointmentQueryEvaluator.java java 12 Lines 2.3 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/service/AppointmentQueryService.java java 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/reporting/query/service/AppointmentQueryServiceImpl.java java 4 Lines 1.9 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/serialize/AppointmentStatusSerializer.java java 4 Lines 1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentBlockValidator.java java 8 Lines 4 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentRequestValidator.java java 5 Lines 2 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentStatusHistoryValidator.java java 5 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentTypeValidator.java java 15 Lines 4.3 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentValidator.java java 7 Lines 3 KB Dec 13, 2019 12:56:58 PM
api/src/main/java/org/openmrs/module/appointmentscheduling/validator/TimeSlotValidator.java java 5 Lines 2.4 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/Appointment.hbm.xml xml 2.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/AppointmentBlock.hbm.xml xml 1.9 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/AppointmentRequest.hbm.xml xml 3.2 KB Dec 13, 2019 12:56:58 PM

api/src/main/resources/AppointmentStatusHistory.hbm.xml xml 1.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/AppointmentType.hbm.xml xml 1.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/TimeSlot.hbm.xml xml 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/liquibase.xml xml 19.2 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/messages.properties java_properties 21.7 KB Dec 13, 2019 12:56:58 PM
api/src/main/resources/moduleApplicationContext.xml xml 6.8 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/AppointmentTest.java java 25 Lines 2 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentBlockServiceTest.java java 173 Lines 19.2 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentRequestServiceTest.java java 106 Lines 13.4 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentServiceTest.java java 259 Lines 24.5 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentStatusHistoryServiceTest.java java 84 Lines 11.1 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentTypeServiceTest.java java 82 Lines 13.4 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/AppointmentUtilityTest.java java 23 Lines 3.5 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/api/TimeSlotServiceTest.java java 165 Lines 18.5 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentCancelReasonDataEvaluatorTest.java java 4 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentEndDateDataEvaluatorTest.java java 5 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentLocationDataEvaluatorTest.java java 4 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentProviderDataEvaluatorTest.java java 4 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentReasonDataEvaluatorTest.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentStartDateDataEvaluatorTest.java java 5 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentStatusDataEvaluatorTest.java java 4 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/AppointmentTypeDataEvaluatorTest.java java 5 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/PatientToAppointmentDataEvaluatorTest.java java 15 Lines 3.5 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/data/evaluator/PersonToAppointmentDataEvaluatorTest.java java 15 Lines 3.3 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/dataset/evaluator/AppointmentDataSetEvaluatorTest.java java 8 Lines 2.2 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/reporting/query/evaluator/BasicAppointmentQueryEvaluatorTest.java java 18 Lines 4.6 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/validator/AppointmentBlockValidatorComponentTest.java java 32 Lines 5.1 KB Dec 13, 2019 12:56:58 PM
api/src/test/java/org/openmrs/module/appointmentscheduling/validator/AppointmentTypeValidatorTest.java java 23 Lines 4 KB Dec 13, 2019 12:56:58 PM
api/src/test/resources/TestingApplicationContext.xml xml 1.1 KB Dec 13, 2019 12:56:58 PM
api/src/test/resources/standardAppointmentTestDataset.xml xml 13.1 KB Dec 13, 2019 12:56:58 PM

api/src/test/resources/test-hibernate.cfg.xml xml Dec 13, 2019 12:56:58 PM
api/target/classes/Appointment.hbm.xml xml 2.2 KB Dec 18, 2019 11:53:40 AM
api/target/classes/AppointmentBlock.hbm.xml xml 1.9 KB Dec 18, 2019 11:53:41 AM
api/target/classes/AppointmentRequest.hbm.xml xml 3.2 KB Dec 18, 2019 11:53:41 AM
api/target/classes/AppointmentStatusHistory.hbm.xml xml 1.2 KB Dec 18, 2019 11:53:41 AM
api/target/classes/AppointmentType.hbm.xml xml 1.7 KB Dec 18, 2019 11:53:40 AM
api/target/classes/TimeSlot.hbm.xml xml 1.6 KB Dec 18, 2019 11:53:40 AM
api/target/classes/liquibase.xml xml 19.2 KB Dec 18, 2019 11:53:41 AM
api/target/classes/messages.properties java_properties 20 KB Dec 18, 2019 11:53:41 AM
api/target/classes/moduleApplicationContext.xml xml 6.7 KB Dec 18, 2019 11:53:40 AM
api/target/maven-archiver/pom.properties java_properties Dec 18, 2019 11:54:27 AM
omod/pom.xml xml 6.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/extension/html/AdminList.java java 11 Lines 2.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/extension/html/AppointmentsHeaderLinkExt.java java 4 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/extension/html/PatientDashboardAppointmentExt.java java 24 Lines 5.6 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/extension/html/PatientDashboardAppointmentTabExt.java java 5 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentRestController.java java 3 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentAllowingOverbookResource1_9.java java 3 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentBlockResource1_9.java java 37 Lines 6.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentBlockWithTimeSlotResource1_9.java java 19 Lines 3.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentRequestResource1_9.java java 39 Lines 8.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentRequestStatusResource1_9.java java 8 Lines 1.8 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentResource1_9.java java 66 Lines 10.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentStatusResource1_9.java java 9 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentStatusTypeResource1_9.java java 8 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentTypeResource1_9.java java 18 Lines 4.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/TimeFrameUnitsResource1_9.java java 8 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/TimeSlotResource1_9.java java 43 Lines 7.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/util/AppointmentRestUtils.java java 8 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/AppointmentBlockData.java java 32 Lines 2.3 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/AppointmentBlockEditor.java java 14 Lines 2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/AppointmentData.java java 20 Lines 1.4 KB Dec 13, 2019

12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/AppointmentEditor.java java 14 Lines 1.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/AppointmentTypeEditor.java java 14 Lines 1.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/DWRAppointmentService.java java 167 Lines 20 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/PatientData.java java 14 Lines 1.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/ProviderEditor.java java 14 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/TimeSlotEditor.java java 14 Lines 1.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentBlockCalendarController.java java 61 Lines 8.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentBlockFormController.java java 102 Lines 14.3 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentBlockListController.java java 88 Lines 12.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentFormController.java java 68 Lines 9.8 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentListController.java java 126 Lines 14.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentSettingsFormController.java java 64 Lines 7.8 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentStatisticsFormController.java java 3 Lines 1.6 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentTypeFormController.java java 24 Lines 4.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentTypeListController.java java 5 Lines 1.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/AppointmentsPortletController.java java 9 Lines 2.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/java/org/openmrs/module/appointmentscheduling/web/controller/PatientDashboardAppointmentExtController.java java 14 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/resources/config.xml xml 9.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/resources/webModuleApplicationContext.xml xml 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentBlockCalendar.jsp jsp 133 Lines 13.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentBlockForm.jsp jsp 172 Lines 18.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentBlockList.jsp jsp 236 Lines 25 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentForm.jsp jsp 216 Lines 23.3 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentList.jsp jsp 45 Lines 22.8 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentSettingsForm.jsp jsp 35 Lines 10.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentStatisticsForm.jsp jsp 9 Lines 19.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentTypeForm.jsp jsp 20 Lines 4.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/appointmentTypeList.jsp jsp 36 Lines 3.6 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/localHeader.jsp jsp 8 Lines 1.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/portlets/appointments.jsp jsp 69 Lines 6.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/date.format.js typescript 68 Lines 3.8 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/fullcalendar.js typescript 2,639 Lines 125.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/fullcalendar.min.js typescript 2 Lines 48.2 KB Dec 13, 2019 12:56:58 PM

omod/src/main/webapp/resources/Scripts/gcal.js typescript 53 Lines 2.6 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.barRenderer.min.js typescript 1 Lines 13.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.categoryAxisRenderer.min.js typescript 1 Lines 9.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.donutRenderer.min.js typescript 1 Lines 12.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.highlighter.js typescript 179 Lines 21.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.pieRenderer.min.js typescript 1 Lines 13.3 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jqPlot-plugins/jqplot.pointLabels.min.js typescript 1 Lines 4.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jquery-ui-1.10.2.custom.min.js typescript 1 Lines 47.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jquery.dataTables.js typescript 2,644 Lines 368.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jquery.jqplot.min.js typescript 1 Lines 168.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/jquery.maxlength.js typescript 38 Lines 2.9 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/json2.js typescript 109 Lines 17.1 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/opentip-jquery-excanvas.js typescript 1,541 Lines 85.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/queryParameters.js typescript 5 Lines Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/statusButtons.js typescript 65 Lines 2.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/Scripts/timepicker.js typescript 35 Lines 1.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as actionscript 32 Lines 3.2 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/TableTools/media/ZeroClipboard/ZeroClipboard.js typescript 148 Lines 9.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/TableTools/media/js/TableTools.js typescript 197 Lines 13.7 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/TableTools/media/support/jquery.dataTables.min.js typescript 442 Lines 53.4 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/resources/TableTools/media/support/jquery.jeditable.js typescript 231 Lines 23.5 KB Dec 13, 2019 12:56:58 PM
omod/src/main/webapp/template/localHeader.jsp jsp 4 Lines Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentAllowingOverbookResource1_9ControllerTest.java java 9 Lines 2.4 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentBlockResource1_9ControllerTest.java java 58 Lines 12.3 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentBlockWithTimeSlotResource1_9ControllerTest.java java 21 Lines 3.7 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentRequestResource1_9ControllerTest.java java 45 Lines 10.6 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentResource1_9ControllerTest.java java 78 Lines 10.8 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/AppointmentTypeResource1_9ControllerTest.java java 49 Lines 7.8 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/controller/TimeSlotResource1_9ControllerTest.java java 67 Lines 12 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentBlockResource1_9Test.java java 4 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentBlockWithTimeSlotResource1_9Test.java java 4 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentRequestResource1_9Test.

java java 4 Lines 2.8 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentResource1_9Test.java java 4 Lines 2 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentStatusResource1_9Test.java java 8 Lines 1.2 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/AppointmentTypeResource1_9Test.java java 4 Lines 2 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/resource/openmrs1_9/TimeSlotResource1_9Test.java java 4 Lines 2.1 KB Dec 13, 2019 12:56:58 PM
omod/src/test/java/org/openmrs/module/appointmentscheduling/rest/test/SameDatetimeMatcher.java java 9 Lines 1.3 KB Dec 13, 2019 12:56:58 PM
omod/src/test/resources/TestingApplicationContext.xml xml 1.1 KB Dec 13, 2019 12:56:58 PM
omod/src/test/resources/standardWebAppointmentTestDataset.xml xml 11.8 KB Dec 13, 2019 12:56:58 PM
omod/src/test/resources/test-hibernate.cfg.xml xml Dec 13, 2019 12:56:58 PM
omod/target/appointmentscheduling-1.10.0/Appointment.hbm.xml xml 2.2 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/AppointmentBlock.hbm.xml xml 1.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/AppointmentRequest.hbm.xml xml 3.2 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/AppointmentStatusHistory.hbm.xml xml 1.2 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/AppointmentType.hbm.xml xml 1.7 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/META-INF/maven/org.openmrs.module/appointmentscheduling-api/pom.properties java_properties Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/META-INF/maven/org.openmrs.module/appointmentscheduling-api/pom.xml xml 1.4 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/TimeSlot.hbm.xml xml 1.6 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/config.xml xml 9.2 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/liquibase.xml xml 19.2 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/messages.properties java_properties 20 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/moduleApplicationContext.xml xml 6.7 KB Dec 18, 2019 11:55:36 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockCalendar.jsp jsp 133 Lines 13.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockForm.jsp jsp 172 Lines 18.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockList.jsp jsp 236 Lines 25 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentForm.jsp jsp 216 Lines 23.3 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentList.jsp jsp 45 Lines 22.8 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentSettingsForm.jsp jsp 35 Lines 10.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentStatisticsForm.jsp jsp 9 Lines 19.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeForm.jsp jsp 20 Lines 4.5 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeList.jsp jsp 36 Lines 3.6 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/localHeader.jsp jsp 8 Lines 1.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/portlets/appointments.jsp jsp 69 Lines 6.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/date.format.js typescript 68 Lines 3.8 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/fullcalendar.js typescript 2,639 Lines 125.4 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/fullcalendar.min.js typescript 2 Lines 48.2 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/gcal.js typescript 53 Lines 2.6 KB Dec 18, 2019 11:55:37 AM

omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.barRenderer.min.js typescript 1 Lines 13.1 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.categoryAxisRenderer.min.js typescript 1 Lines 9.5 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.donutRenderer.min.js typescript 1 Lines 12.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.highlighter.js typescript 179 Lines 21.4 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.pieRenderer.min.js typescript 1 Lines 13.3 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jqPlot-plugins/jqplot.pointLabels.min.js typescript 1 Lines 4.5 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jquery-ui-1.10.2.custom.min.js typescript 1 Lines 47.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jquery.dataTables.js typescript 2,644 Lines 368.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jquery.jqplot.min.js typescript 1 Lines 168.4 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/jquery.maxlength.js typescript 38 Lines 2.9 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/json2.js typescript 109 Lines 17.1 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/opentip-jquery-excanvas.js typescript 1,541 Lines 85.4 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/queryParameters.js typescript 5 Lines Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/statusButtons.js typescript 65 Lines 2.2 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/Scripts/timepicker.js typescript 35 Lines 1.5 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as actionscript 32 Lines 3.2 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.js typescript 148 Lines 9.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/js/TableTools.js typescript 197 Lines 13.7 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/support/jquery.dataTables.min.js typescript 442 Lines 53.4 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/support/jquery.jeditable.js typescript 231 Lines 23.5 KB Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/web/module/template/localHeader.jsp jsp 4 Lines Dec 18, 2019 11:55:37 AM
omod/target/appointmentscheduling-1.10.0/webModuleApplicationContext.xml xml 2.1 KB Dec 18, 2019 11:55:36 AM
omod/target/classes/Appointment.hbm.xml xml 2.2 KB Dec 18, 2019 11:53:40 AM
omod/target/classes/AppointmentBlock.hbm.xml xml 1.9 KB Dec 18, 2019 11:53:42 AM
omod/target/classes/AppointmentRequest.hbm.xml xml 3.2 KB Dec 18, 2019 11:53:42 AM
omod/target/classes/AppointmentStatusHistory.hbm.xml xml 1.2 KB Dec 18, 2019 11:53:42 AM
omod/target/classes/AppointmentType.hbm.xml xml 1.7 KB Dec 18, 2019 11:53:40 AM
omod/target/classes/META-INF/maven/org.openmrs.module/appointmentscheduling-api/pom.properties java_properties Dec 18, 2019 11:54:28 AM
omod/target/classes/META-INF/maven/org.openmrs.module/appointmentscheduling-api/pom.xml xml 1.4 KB Dec 13, 2019 12:56:58 PM

omod/target/classes/TimeSlot.hbm.xml xml 1.6 KB Dec 18, 2019 11:53:40 AM
omod/target/classes/config.xml xml 9.2 KB Dec 18, 2019 11:55:00 AM
omod/target/classes/liquibase.xml xml 19.2 KB Dec 18, 2019 11:53:42 AM
omod/target/classes/messages.properties java_properties 20 KB Dec 18, 2019 11:53:42 AM
omod/target/classes/moduleApplicationContext.xml xml 6.7 KB Dec 18, 2019 11:53:40 AM
omod/target/classes/web/module/appointmentBlockCalendar.jsp jsp 133 Lines 13.7 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/appointmentBlockForm.jsp jsp 172 Lines 18.9 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/appointmentBlockList.jsp jsp 236 Lines 25 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/appointmentForm.jsp jsp 216 Lines 23.3 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/appointmentList.jsp jsp 45 Lines 22.8 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/appointmentSettingsForm.jsp jsp 35 Lines 10.9 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/appointmentStatisticsForm.jsp jsp 9 Lines 19.9 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/appointmentTypeForm.jsp jsp 20 Lines 4.5 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/appointmentTypeList.jsp jsp 36 Lines 3.6 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/localHeader.jsp jsp 8 Lines 1.7 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/portlets/appointments.jsp jsp 69 Lines 6.9 KB Dec 18, 2019 11:55:02 AM
omod/target/classes/web/module/resources/Scripts/date.format.js typescript 68 Lines 3.8 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/fullcalendar.js typescript 2,639 Lines 125.4 KB Dec 18, 2019 11:55:03 AM
omod/target/classes/web/module/resources/Scripts/fullcalendar.min.js typescript 2 Lines 48.2 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/gcal.js typescript 53 Lines 2.6 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.barRenderer.min.js typescript 1 Lines 13.1 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.categoryAxisRenderer.min.js typescript 1 Lines 9.5 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.donutRenderer.min.js typescript 1 Lines 12.9 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.highlighter.js typescript 179 Lines 21.4 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.pieRenderer.min.js typescript 1 Lines 13.3 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jqPlot-plugins/jqplot.pointLabels.min.js typescript 1 Lines 4.5 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jquery-ui-1.10.2.custom.min.js typescript 1 Lines 47.7 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jquery.dataTables.js typescript 2,644 Lines 368.7 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/jquery.jqplot.min.js typescript 1 Lines 168.4 KB Dec 18, 2019 11:55:03 AM
omod/target/classes/web/module/resources/Scripts/jquery.maxlength.js typescript 38 Lines 2.9 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/json2.js typescript 109 Lines 17.1 KB Dec 18, 2019 11:55:03 AM
omod/target/classes/web/module/resources/Scripts/opentip-jquery-excanvas.js typescript 1,541 Lines 85.4 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/queryParameters.js typescript 5 Lines Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/resources/Scripts/statusButtons.js typescript 65 Lines 2.2 KB Dec 18, 2019 11:55:03 AM
omod/target/classes/web/module/resources/Scripts/timepicker.js typescript 35 Lines 1.5 KB Dec 18, 2019 11:55:03 AM
omod/target/classes/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as actionscript 32 Lines 3.2 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.js typescript 148 Lines 9.7 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/resources/TableTools/media/js/TableTools.js typescript 197 Lines 13.7 KB Dec 18, 2019 11:55:05 AM
omod/target/classes/web/module/resources/TableTools/media/support/jquery.dataTables.min.js typescript 442 Lines 53.4 KB Dec 18, 2019 11:55:04 AM

omod/target/classes/web/module/resources/TableTools/media/support/jquery.jeditable.js typescript 231 Lines 23.5 KB Dec 18, 2019 11:55:04 AM
omod/target/classes/web/module/template/localHeader.jsp jsp 4 Lines Dec 18, 2019 11:55:02 AM
omod/target/classes/webModuleApplicationContext.xml xml 2.1 KB Dec 18, 2019 11:55:00 AM
omod/target/maven-archiver/pom.properties java_properties Dec 18, 2019 11:55:31 AM
pom.xml xml 6.5 KB Dec 13, 2019 12:56:58 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Core, Java
Version: 2019.4.0.0009
ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF
SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, Annotations
Version: 2019.4.0.0009
ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B
SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, ActionScript 3.0
Version: 2019.4.0.0009
ID: 92127AA2-E666-4F28-B1C1-C0F6A939A089
SKU: RUL13094

Name: Fortify Secure Coding Rules, Core, JavaScript
Version: 2019.4.0.0009
ID: BD292C4E-4216-4DB8-96C7-9B607BFD9584
SKU: RUL13059

Name: Fortify Secure Coding Rules, Core, Android
Version: 2019.4.0.0009
ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952
SKU: RUL13093

Name: Fortify Secure Coding Rules, Extended, JavaScript
Version: 2019.4.0.0009
ID: C4D1969E-B734-47D3-87D4-73962C1D32E2
SKU: RUL13141

Name: Fortify Secure Coding Rules, Extended, Configuration

Version: 2019.4.0.0009
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Java
Version: 2019.4.0.0009
ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317
SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2019.4.0.0009
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

Name: Fortify Secure Coding Rules, Core, Golang
Version: 2019.4.0.0009
ID: 1DCE79F8-AF6B-474D-A05A-5BFFC8B13DCD
SKU: RUL13218

Name: Fortify Secure Coding Rules, Extended, JSP
Version: 2019.4.0.0009
ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2
SKU: RUL13026

External Metadata:
Version: 2019.4.0.0009

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hiearchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like langauges and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard

identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA

The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE
The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007
ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248
The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0
ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at

project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden

or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].

DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4

ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5
ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930:

CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8
ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.X11.XToolkit
com.fortify.AuthenticationKey=/home/pgupta25/.fortify/config/tools
com.fortify.Core=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core
com.fortify.InstallRoot=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0
com.fortify.InstallationUserName=pgupta25
com.fortify.SCAExecutablePath=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/bin/sourceanalyzer
com.fortify.TotalPhysicalMemory=8363917312
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=/home/pgupta25/.fortify
com.fortify.locale=en
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=appointmentscheduling
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer
com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settings,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshtml,vbhtml,inc,asp,vbscript,js,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,conf,json,yaml,yml
com.fortify.sca.DefaultJarsDirs=default_jars

com.fortify.sca.DefaultRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/rules
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PHPLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFileDir=/home/pgupta25/.fortify/sca19.1/log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=/home/pgupta25/.fortify/sca19.1/log/sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshtml,vbhtml
com.fortify.sca.PID=30642
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=/srv/openmrs_code/org/openmrs/module/appointmentscheduling/appointmentscheduling_scan.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=PLSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs

com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fi
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.cpfe.441.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.abap=ABAP

com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP
com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP
com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT

com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4
com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
file.encoding=UTF-8
file.encoding.pkg=sun.io
file.separator=/
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.print.PSPrinterJob
java.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/endorsed
java.ext.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/ext:/usr/java/packages/lib/ext
java.home=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre
java.io.tmpdir=/tmp
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation

java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/log4j2.xml
log4j.isThreadContextMapInheritable=true
max.file.path.length=255
os.arch=amd64
os.name=Linux
os.version=4.15.0-58-generic
path.separator=:
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/resources.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/rt.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/sunrsasign.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jsse.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jce.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/charsets.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jfr.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/classes
sun.boot.library.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/amd64
sun.cpu.endian=little
sun.cpu.isalist=
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:SoftRefLRUPolicyMSPerMB=3000 -Dcom.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin -Dcom.fortify.sca.ProjectRoot=/home/pgupta25/.fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=30642 -Xmx4096M -Dcom.fortify.TotalPhysicalMemory=8363917312 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M -Djava.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar -scan @/home/pgupta25/.fortify/Eclipse.Plugin-19.1.0/appointmentscheduling/appointmentschedulingScan.txt
sun.jnu.encoding=UTF-8
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=unknown
user.country=US
user.dir=/home/pgupta25
user.home=/home/pgupta25
user.language=en
user.name=pgupta25
user.timezone=America/New_York

Commandline Arguments

-scan
-b
appointmentscheduling
-format
fpr
-machine-output
-f
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/appointmentscheduling_scan.fpr

Warnings

[12002] Could not locate the deployment descriptor (web.xml) for your web application. Please build your web application and try again. File: /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockCalendar.jsp
[12003] Assuming Java source level to be 1.8 as it was not specified. Note that the default value may change in future versions.
[12004] The Java frontend was unable to resolve the following include: /WEB-INF/template/include.jsp at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/portlets/appointments.jsp:1. /WEB-INF/template/footer.jsp at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp:530. /WEB-INF/template/header.jsp at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp:2.
[12004] The ActionScript frontend was unable to resolve the following import: flash.display at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:2. flash.events at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:6. flash.net at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:13. flash.external at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:9. flash.system at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:10. flash.utils at /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/resources/TableTools/media/ZeroClipboard/ZeroClipboard.as:11.
[12010] You may need to specify additional SWC or SWF Flex libraries (-flex-libraries option, or com.fortify.sca.FlexLibraries property)
[12022] The class "javax.servlet.http.HttpServlet" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet-api-3.0.1.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.http.HttpServlet" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[12022] The class "javax.servlet.jsp.PageContext" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet.jsp-api.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.jsp.PageContext" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[1214] Multiple definitions found for class /appointmentBlockCalendar.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockCalendar.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockCalendar.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockCalendar_jsp$ftfy_frameworkVisibleObjects

(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockCalendar.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockCalendar.jsp).
[1214] Multiple definitions found for class /appointmentBlockForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockForm.jsp).
[1214] Multiple definitions found for class /appointmentBlockList.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentBlockList.jsp).
[1214] Multiple definitions found for class /appointmentForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentForm.jsp).
[1214] Multiple definitions found for class /appointmentList.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentList.jsp).
[1214] Multiple definitions found for class /appointmentSettingsForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentSettingsForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentSettingsForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentSettingsForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentSettingsForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentSettingsForm.jsp).
[1214] Multiple definitions found for class /appointmentStatisticsForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentStatisticsForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentStatisticsForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentStatisticsForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentStatisticsForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentStatisticsForm.jsp).

[1214] Multiple definitions found for class /appointmentTypeForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentTypeForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeForm.jsp).
[1214] Multiple definitions found for class /appointmentTypeList.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentTypeList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/appointmentTypeList.jsp).
[1214] Multiple definitions found for class /appointments.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/portlets/appointments.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/portlets/appointments.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointments_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/portlets/appointments.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/portlets/appointments.jsp).
[1214] Multiple definitions found for class /localHeader.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/template/localHeader.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/template/localHeader.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsplocalHeader_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/template/localHeader.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/appointmentscheduling-1.10.0/web/module/template/localHeader.jsp).
[1214] Multiple definitions found for class /appointmentBlockCalendar.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockCalendar.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockCalendar.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockCalendar_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockCalendar.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockCalendar.jsp).
[1214] Multiple definitions found for class /appointmentBlockForm.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockForm.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockForm.jsp).
[1214] Multiple definitions found for class /appointmentBlockList.jsp (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp and /srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentBlockList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentBlockList.jsp and

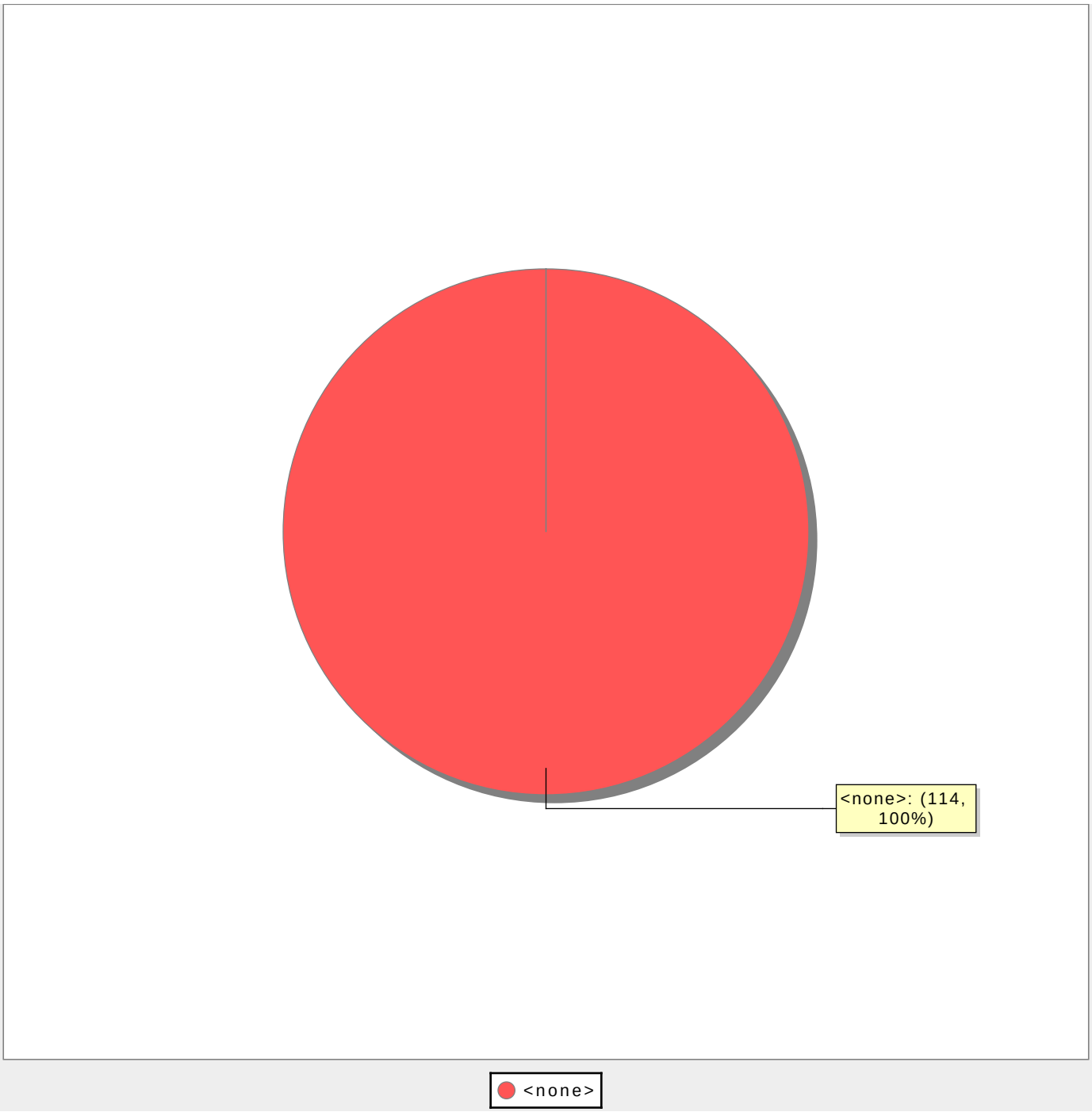
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentBlockList.jsp).
[1214] Multiple definitions found for class /appointmentForm.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentForm.jsp).
[1214] Multiple definitions found for class /appointmentList.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentList.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentList.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentList.jsp).
[1214] Multiple definitions found for class /appointmentSettingsForm.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentSettingsForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentSettingsForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentSettingsForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentSettingsForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentSettingsForm.jsp).
[1214] Multiple definitions found for class /appointmentStatisticsForm.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentStatisticsForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentStatisticsForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentStatisticsForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentStatisticsForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentStatisticsForm.jsp).
[1214] Multiple definitions found for class /appointmentTypeForm.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentTypeForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentTypeForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeForm.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentTypeForm.jsp).
[1214] Multiple definitions found for class /appointmentTypeList.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeList.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentTypeList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointmentTypeList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/appointmentTypeList.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/appointmentTypeList.jsp).
[1214] Multiple definitions found for class /appointments.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/portlets/appointments.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/portlets/appointments.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspappointments_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/portlets/appointments.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/portlets/appointments.jsp).
[1214] Multiple definitions found for class /localHeader.jsp
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/template/localHeader.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/template/localHeader.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsplocalHeader_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/src/main/webapp/template/localHeader.jsp and
/srv/openmrs_code/org/openmrs/module/appointmentscheduling/omod/target/classes/web/module/template/localHeader.jsp).
[1215] Could not locate the root (WEB-INF) of the web application. Please build your web application and try again.

Issue Count by Category

Issues by Category	
Cross-Site Scripting: DOM	54
Cross-Site Scripting: Reflected	36
Header Manipulation: Cookies	12
Dynamic Code Evaluation: Code Injection	6
Key Management: Hardcoded Encryption Key	3
Open Redirect	3

Issue Breakdown by Analysis

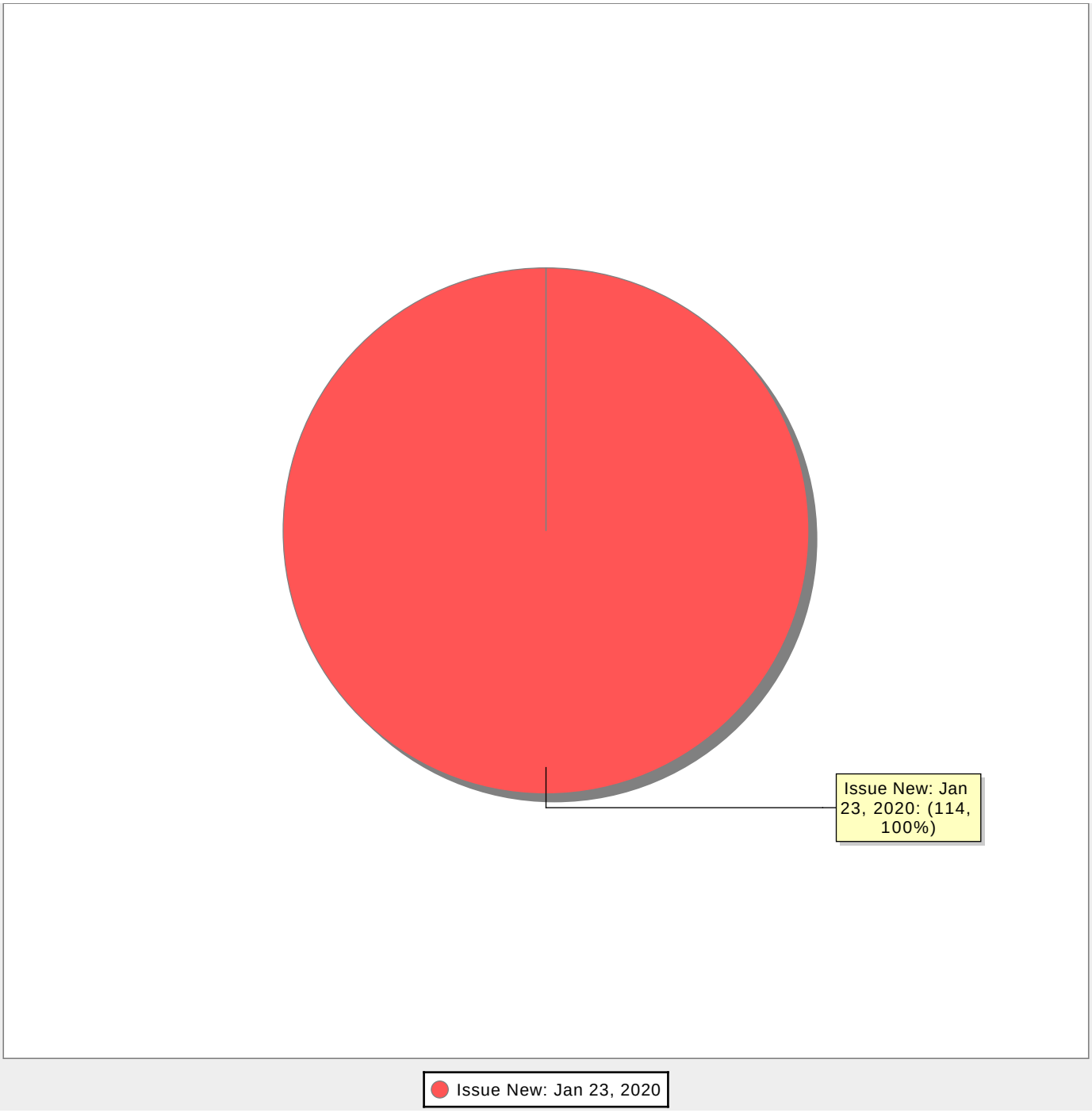
Issues by Analysis



New Issues

Issues by New Issue

The following issues have been discovered since the last scan.



Fortify Security Report

Jan 22, 2020

pgupta25

Executive Summary

Issues Overview

On Jan 22, 2020, a source code review was performed over the calculation code base. 119 files, 6,179 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 78 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
Critical	72
High	6

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: /srv/openmrs_code/org/openmrs/module/calculation
Number of Files: 119
Lines of Code: 6179
Build Label: <No Build Label>

Scan Information

Scan time: 12:27
SCA Engine version: 19.1.0.2241
Machine Name: vclv99-89.hpc.ncsu.edu
Username running scan: pgupta25

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Private Information:
null.null.null

System Information:
null.null.null
java.io.File.listFiles
java.lang.ClassLoader.getResource
java.lang.Throwable.getMessage

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium

If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
If impact is not in range [2.5, 5.0] Then hide issue
If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

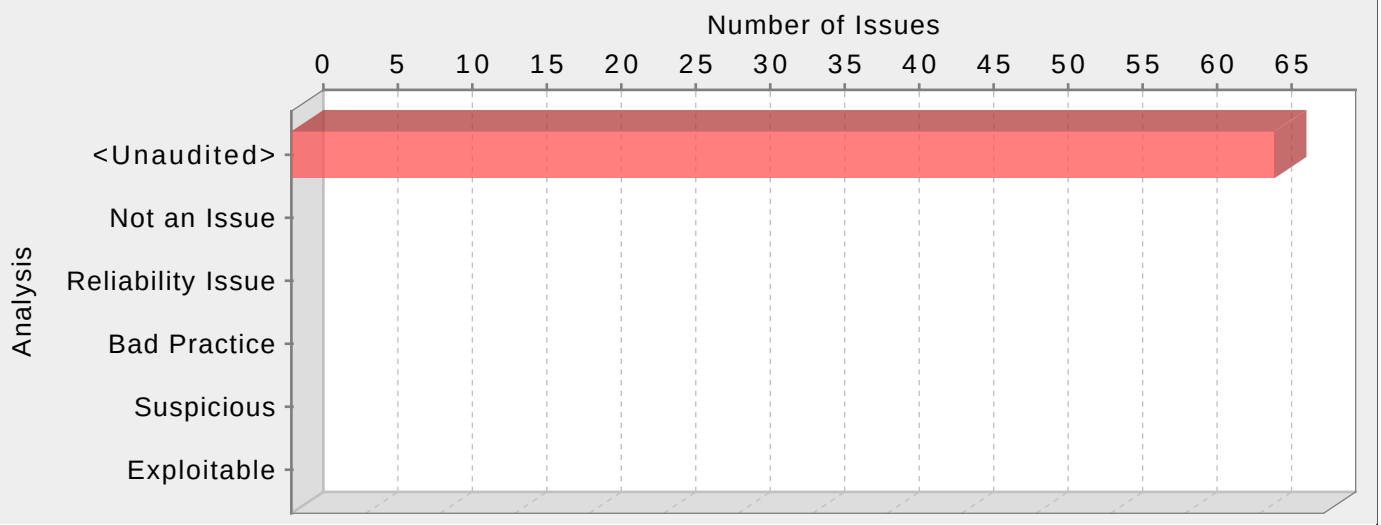
Results Outline

Overall number of results

The scan found 78 issues.

Vulnerability Examples by Category

Category: Cross-Site Scripting: DOM (66 Issues)



Abstract:

The method _fnAddData() in jquery.dataTables.js sends unvalidated data to a web browser on line 1704, which can result in the browser executing malicious code.

Explanation:

Cross-site scripting (XSS) vulnerabilities occur when:

1. Data enters a web application through an untrusted source. In the case of DOM-based XSS, data is read from a URL parameter or other value within the browser and written back into the page with client-side code. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store.

2. The data is included in dynamic content that is sent to a web user without being validated. In the case of DOM Based XSS, malicious content gets executed as part of DOM (Document Object Model) creation, whenever the victim's browser parses the HTML page.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Example 1: The following JavaScript code segment reads an employee ID, eid, from a URL and displays it to the user.

```
<SCRIPT>
var pos=document.URL.indexOf("eid=")+4;
document.write(document.URL.substring(pos,document.URL.length));
</SCRIPT>
```

Example 2: Consider the HTML form:

```
<div id="myDiv">
Employee ID: <input type="text" id="eid"><br>
...
<button>Show results</button>
</div>
<div id="resultsDiv">
...
</div>
```

The following jQuery code segment reads an employee ID from the form, and displays it to the user.

```
$(document).ready(function(){
$("#myDiv").on("click", "button", function(){
var eid = $("#eid").val();
$("resultsDiv").append(eid);
...
});
});
```

These code examples operate correctly if the employee ID, from the text input with ID eid contains only standard alphanumeric text. If eid has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Example 3: The following code shows an example of a DOM-based XSS within a React application:

```
let element = JSON.parse(getUntrustedInput());
ReactDOM.render(<App>
{element}
</App>);
```

In Example 3, if an attacker can control the entire JSON object retrieved from getUntrustedInput(), they may be able to make React render element as a component, and therefore can pass an object with dangerouslySetInnerHTML with their own controlled value, a typical cross-site scripting attack.

Initially these might not appear to be much of a vulnerability. After all, why would someone provide input containing malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS.

As the example demonstrates, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim:

- Data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities.

- The application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

- A source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

Recommendations:

The solution to XSS is to ensure that validation occurs in the correct places and checks are made for the correct properties.

Since XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user.

The most secure approach to validation for XSS is to create a whitelist of safe characters that are allowed to appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alpha-numeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser should still be considered valid input once they are encoded, such as a web design bulletin board that must accept HTML fragments from its users.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines what characters have special meaning, many web browsers try to correct common mistakes in HTML and may treat other characters as special in certain contexts, which is why we do not encourage the use of blacklists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]:

In the content of a block-level element (in the middle of a paragraph of text):

- "<" is special because it introduces a tag.

- "&" is special because it introduces a character entity.

- ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error.

The following principles apply to attribute values:

- In attribute values enclosed with double quotes, the double quotes are special because they mark the end of the attribute value.

- In attribute values enclosed with single quote, the single quotes are special because they mark the end of the attribute value.

- In attribute values without any quotes, white-space characters, such as space and tab, are special.

- "&" is special when used with certain attributes, because it introduces a character entity.

In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters:

- Space, tab, and new line are special because they mark the end of the URL.

- "&" is special because it either introduces a character entity or separates CGI parameters.

- Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context.

- The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server -side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page in question.

Within the body of a <SCRIPT> </SCRIPT>:

- Semicolons, parentheses, curly braces, and new line characters should be filtered out in situations where text could be inserted directly into a pre-existing script tag.

Server-side scripts:

- Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering.

Other possibilities:

- If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and may bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7).

After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option in this situation is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and may be unacceptable in circumstances where the integrity of the input must be preserved for display.

If input containing special characters must be accepted and displayed accurately, validation must encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2].

Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

Tips:

1. The Fortify Secure Coding Rulepacks warn about SQL Injection and Access Control: Database issues when untrusted data is written to a database and also treat the database as a source of untrusted data, which can lead to XSS vulnerabilities. If the database is a trusted resource in your environment, use custom filters to filter out dataflow issues that include the DATABASE taint flag or originate from database sources. Nonetheless, it is often still a good idea to validate everything read from the database.

2. Even though URL encoding untrusted data protects against many XSS attacks, some browsers (specifically, Internet Explorer 6 and 7 and possibly others) automatically decode content at certain locations within the Document Object Model (DOM) prior to passing it to the JavaScript interpreter. To reflect this danger, the rulepacks no longer treat URL encoding routines as sufficient to protect against cross-site scripting. Data values that are URL encoded and subsequently output will cause Fortify to report Cross-Site Scripting: Poor Validation vulnerabilities.

3. Older versions of React are more susceptible to cross-site scripting attacks by controlling an entire component. Newer versions use Symbols to identify a React component, which prevents the exploit, however older browsers that do not have Symbol support (natively, or through polyfills), such as all versions of Internet Explorer, are still vulnerable. Other types of cross-site scripting attacks are valid for all browsers and versions of React.

jquery.dataTables.js, line 1704 (Cross-Site Scripting: DOM)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The method _fnAddData() in jquery.dataTables.js sends unvalidated data to a web browser on line 1704, which can result in the browser executing malicious code.		

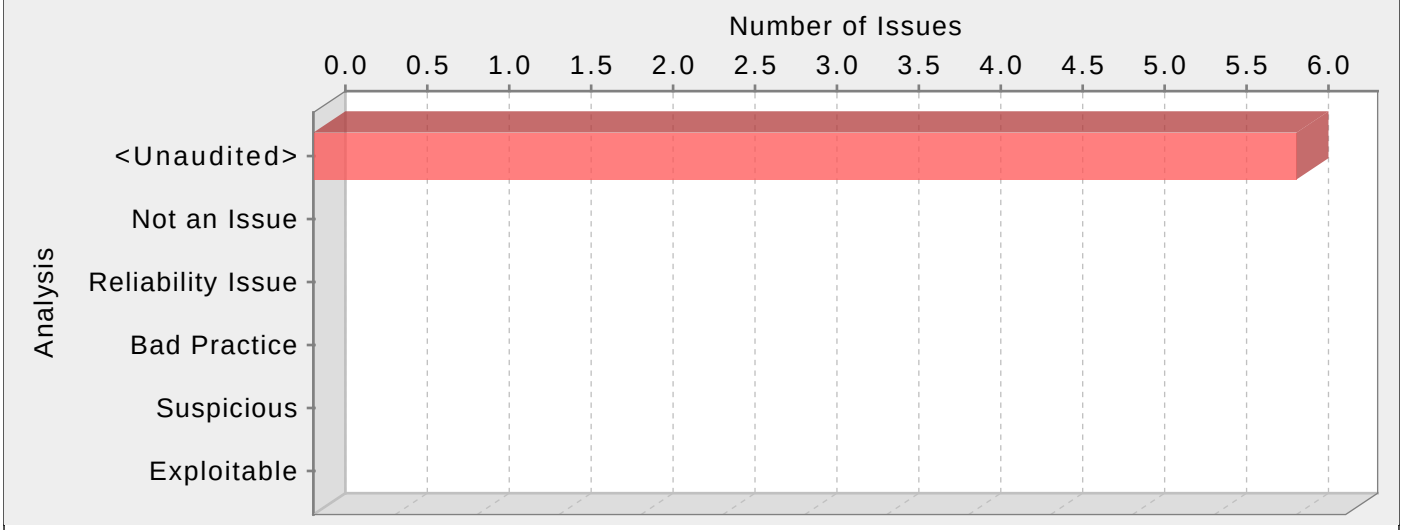
Source: jquery.dataTables.js:1527 lambda(0)

```
1525        _fnProcessingDisplay( oSettings, true );
1526
1527        $.getJSON( oSettings.sAjaxSource, null, function(json) {
1528         /* Got the data - add it to the table */
1529         for ( var i=0 ; i<json.aaData.length ; i++ )
```

Sink: jquery.dataTables.js:1704 Assignment to nTd.innerHTML()

```
1702        else
1703        {
1704         nTd.innerHTML = aData[i];
1705        }
1706
```

Category: Dynamic Code Evaluation: Code Injection (6 Issues)



Abstract:

The file jquery.dataTables.js interprets unvalidated user input as source code on line 3643. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.

Explanation:

Many modern programming languages allow dynamic interpretation of source instructions. This capability allows programmers to perform dynamic instructions based on input received from the user. Code injection vulnerabilities occur when the programmer incorrectly assumes that instructions supplied directly from the user will perform only innocent operations, such as performing simple calculations on active user objects or otherwise modifying the user's state. However, without proper validation, a user might specify operations the programmer does not intend.

Example: In this classic code injection example, the application implements a basic calculator that allows the user to specify commands for execution.

...
userOp = form.operation.value;
calcResult = eval(userOp);
...

The program behaves correctly when the operation parameter is a benign value, such as "8 + 7 * 2", in which case the calcResult variable is assigned a value of 22. However, if an attacker specifies languages operations that are both valid and malicious, those operations would be executed with the full privilege of the parent process. Such attacks are even more dangerous when the underlying language provides access to system resources or allows execution of system commands. In the case of JavaScript, the attacker may utilize this vulnerability to perform a cross-site scripting attack.

Recommendations:

Avoid dynamic code interpretation whenever possible. If your program's functionality requires code to be interpreted dynamically, the likelihood of attack can be minimized by constraining the code your program will execute dynamically as much as possible, limiting it to an application- and context-specific subset of the base programming language.

If dynamic code execution is required, unvalidated user input should never be directly executed and interpreted by the application. Instead, use a level of indirection: create a list of legitimate operations and data objects that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never executed directly.

jquery.dataTables.js, line 3643 (Dynamic Code Evaluation: Code Injection)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file jquery.dataTables.js interprets unvalidated user input as source code on line 3643. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.		

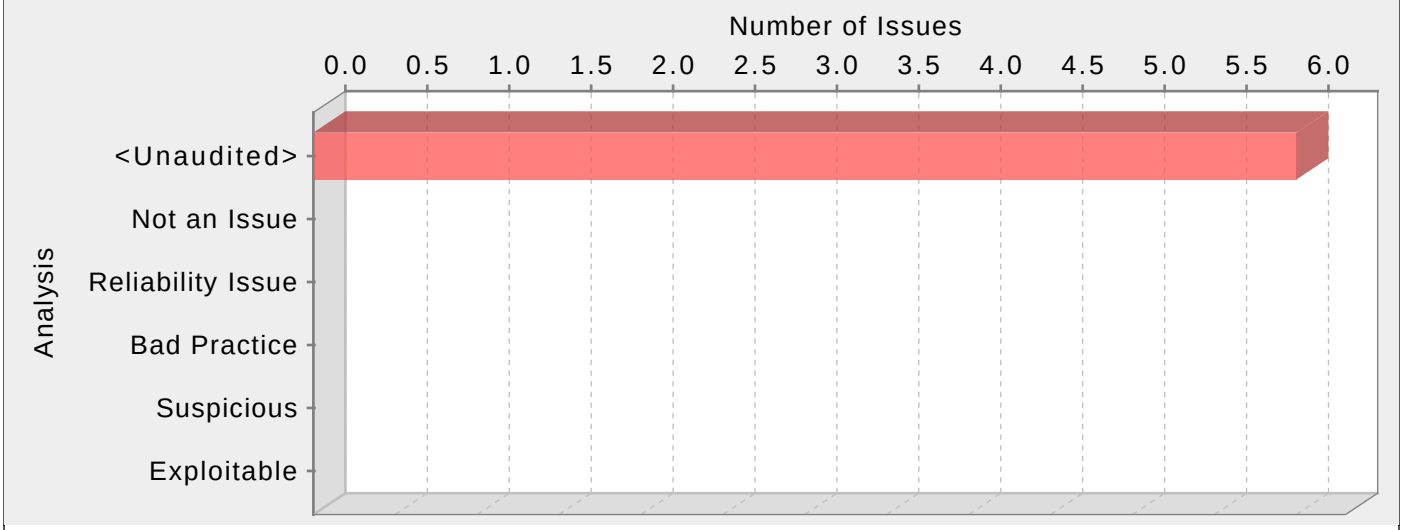
Source: jquery.dataTables.js:3711 Read document.cookie()

```
3709    {
3710      var sNameEQ = sName +'_'+ window.location.pathname.replace(/[\/:]/g,"").toLowerCase()
+ "=";
3711      var sCookieContents = document.cookie.split(';');
3712
3713      for( var i=0 ; i<sCookieContents.length ; i++ )
```

Sink: jquery.dataTables.js:3643 eval()

```
3641                        else
3642                        {
3643                         oData = eval( '('+sData+')' );
3644                        }
3645                       }
```

Category: Header Manipulation: Cookies (6 Issues)



Abstract:

The method _fnCreateCookie() in jquery.dataTables.js includes unvalidated data in an HTTP cookie on line 3699. This enables Cookie manipulation attacks and can lead to other HTTP Response header manipulation attacks like: cache-poisoning, cross-site scripting, cross-user defacement, page hijacking or open redirect.

Explanation:

Cookie Manipulation vulnerabilities occur when:

1. Data enters a web application through an untrusted source, most frequently an HTTP request.

2. The data is included in an HTTP cookie sent to a web user without being validated.

As with many software security vulnerabilities, cookie manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP cookie.

Cookie Manipulation: When combined with attacks like cross-site request forgery, attackers may change, add to, or even overwrite a legitimate user's cookies.

Being an HTTP Response header, Cookie manipulation attacks can also lead to other types of attacks like:

HTTP Response Splitting:

One of the most common Header Manipulation attacks is HTTP Response Splitting. To mount a successful HTTP Response Splitting exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header. These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allows them to create additional responses entirely under their control.

Many of today's modern application servers will prevent the injection of malicious characters into HTTP headers. For example, recent versions of Apache Tomcat will throw an IllegalArgumentException if you attempt to set a header with prohibited characters. If your application server prevents setting headers with new line characters, then your application is not vulnerable to HTTP Response Splitting. However, solely filtering for new line characters can leave an application vulnerable to Cookie Manipulation or Open Redirects, so care must still be taken when setting HTTP headers with user input.

Example: The following code segment reads the name of the author of a weblog entry, author, from an HTTP request and sets it in a cookie header of an HTTP response.

```
author = form.author.value;
...
document.cookie = "author=" + author + ";expires="+cookieExpiration;
...
```

Assuming a string consisting of standard alpha-numeric characters, such as "Jane Smith", is submitted in the request the HTTP response including this cookie might take the following form:

```
HTTP/1.1 200 OK
...
Set-Cookie: author=Jane Smith
...
```

However, because the value of the cookie is formed of unvalidated user input the response will only maintain this form if the value submitted for AUTHOR_PARAM does not contain any CR and LF characters. If an attacker submits a malicious string, such as "Wiley Hacker\r\nHTTP/1.1 200 OK\r\n...", then the HTTP response would be split into two responses of the following form:

HTTP/1.1 200 OK

...
Set-Cookie: author=Wiley Hacker

HTTP/1.1 200 OK

...

Clearly, the second response is completely controlled by the attacker and can be constructed with any header and body content desired. The ability of attacker to construct arbitrary HTTP responses permits a variety of resulting attacks, including: cross-user defacement, web and browser cache poisoning, cross-site scripting, and page hijacking.

Cross-User Defacement: An attacker will be able to make a single request to a vulnerable server that will cause the server to create two responses, the second of which may be misinterpreted as a response to a different request, possibly one made by another user sharing the same TCP connection with the server. This can be accomplished by convincing the user to submit the malicious request themselves, or remotely in situations where the attacker and the user share a common TCP connection to the server, such as a shared proxy server. In the best case, an attacker may leverage this ability to convince users that the application has been hacked, causing users to lose confidence in the security of the application. In the worst case, an attacker may provide specially crafted content designed to mimic the behavior of the application but redirect private information, such as account numbers and passwords, back to the attacker.

Cache Poisoning: The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a response is cached in a shared web cache, such as those commonly found in proxy servers, then all users of that cache will continue receive the malicious content until the cache entry is purged. Similarly, if the response is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is purged, although only the user of the local browser instance will be affected.

Cross-Site Scripting: Once attackers have control of the responses sent by an application, they have a choice of a variety of malicious content to provide users. Cross-site scripting is common form of attack where malicious JavaScript or other code included in a response is executed in the user's browser. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. The most common and dangerous attack vector against users of a vulnerable application uses JavaScript to transmit session and authentication information back to the attacker who can then take complete control of the victim's account.

Page Hijacking: In addition to using a vulnerable application to send malicious content to a user, the same root vulnerability can also be leveraged to redirect sensitive content generated by the server and intended for the user to the attacker instead. By submitting a request that results in two responses, the intended response from the server and the response generated by the attacker, an attacker may cause an intermediate node, such as a shared proxy server, to misdirect a response generated by the server for the user to the attacker. Because the request made by the attacker generates two responses, the first is interpreted as a response to the attacker's request, while the second remains in limbo. When the user makes a legitimate request through the same TCP connection, the attacker's request is already waiting and is interpreted as a response to the victim's request. The attacker then sends a second request to the server, to which the proxy server responds with the server generated request intended for the victim, thereby compromising any sensitive information in the headers or body of the response intended for the victim.

Open Redirect: Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Recommendations:

The solution to cookie manipulation is to ensure that input validation occurs in the correct places and checks for the correct properties.

Since Header Manipulation vulnerabilities like cookie manipulation occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating responses dynamically, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for Header Manipulation.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for Header Manipulation is generally relatively easy. Despite its value, input validation for Header Manipulation does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent Header Manipulation vulnerabilities is to validate everything that enters the application or leaves the application destined for the user.

The most secure approach to validation for Header Manipulation is to create a whitelist of safe characters that are allowed to appear in HTTP response headers and accept input composed exclusively of characters in the approved set. For example, a valid name might only include alpha-numeric characters or an account number might only include digits 0-9.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning in HTTP response headers. Although the CR and LF characters are at the heart of an HTTP response splitting attack, other characters, such as ':' (colon) and '=' (equal), have special meaning in response headers as well.

After you identify the correct points in an application to perform validation for Header Manipulation attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. The application should reject any input destined to be included in HTTP response headers that contains special characters, particularly CR and LF, as invalid.

Many application servers attempt to limit an application's exposure to HTTP response splitting vulnerabilities by providing implementations for the functions responsible for setting HTTP headers and cookies that perform validation for the characters essential to an HTTP response splitting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

jquery.dataTables.js, line 3699 (Header Manipulation: Cookies)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method _fnCreateCookie() in jquery.dataTables.js includes unvalidated data in an HTTP cookie on line 3699. This enables Cookie manipulation attacks and can lead to other HTTP Response header manipulation attacks like: cache-poisoning, cross-site scripting, cross-user defacement, page hijacking or open redirect.		

Source: jquery.dataTables.js:3697 Read window.location()

```
3695                 * have to append the pathname to the cookie name. Appalling.
3696                 */
3697                sName += '_'+window.location.pathname.replace(/[\/:]/g,"").toLowerCase();
3698
3699                document.cookie = sName+"="+sValue+"; expires="+date.toGMTString()+"; path=/";
```

Sink: jquery.dataTables.js:3699 Assignment to document.cookie()

```
3697                sName += '_'+window.location.pathname.replace(/[\/:]/g,"").toLowerCase();
3698
3699                document.cookie = sName+"="+sValue+"; expires="+date.toGMTString()+"; path=/";
3700              }
3701
```

Detailed Project Summary

Files Scanned

Code base location: /srv/openmrs_code/org/openmrs/module/calculation

Files Scanned:

api/pom.xml xml 2 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/BaseCalculation.java java 5 Lines 1.6 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/Calculation.java java 1.1 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationActivator.java java 21 Lines 2.8 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationConstants.java java 6 Lines 1.1 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationContext.java java 1.7 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationProvider.java java 1.7 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationRegistration.java java 25 Lines 3.6 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationRegistrationSuggestion.java java 1.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationRegistrationValidator.java java 10 Lines 3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/CalculationUtil.java java 36 Lines 6.5 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/ClasspathCalculationProvider.java java 9 Lines 2.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/ConfigurableCalculation.java java Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/ConversionException.java java 5 Lines 1.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/EvaluationInstanceData.java java Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/ImplementationConfiguredCalculationProvider.java java 26 Lines 3.1 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/InvalidCalculationException.java java 8 Lines 2 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/InvalidParameterValueException.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/MissingParameterException.java java 5 Lines 1.4 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/api/CalculationRegistrationService.java java 4.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/api/CalculationRegistrationServiceImpl.java java 21 Lines 5 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/db/CalculationRegistrationDAO.java java 2.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/db/HibernateCalculationRegistrationDAO.java java 19 Lines 4.8 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/parameter/ParameterDefinition.java java 1.9 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/parameter/ParameterDefinitionSet.java java 6 Lines 1.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/parameter/SimpleParameterDefinition.java java 29 Lines 4.8 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientAtATimeCalculation.java java 9 Lines 3.5 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientCalculation.java java 1.9 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientCalculationContext.java java Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientCalculationService.java java 4.7 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientCalculationServiceImpl.java java 50 Lines 8.4 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/patient/PatientIdCalculation.java java 5 Lines 1.6 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/CalculationResult.java java 1.5 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/CalculationResultMap.java java 6 Lines 1.9 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/DateBasedResult.java java 1 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/EncounterResult.java java 5 Lines 2 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/ListResult.java java 24 Lines 4.3 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/ObsResult.java java 5 Lines 1.9 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/ResultUtil.java java 43 Lines 8.9 KB Dec 13, 2019 12:56:31 PM

api/src/main/java/org/openmrs/calculation/result/SimpleResult.java java 15 Lines 3.1 KB Dec 13, 2019 12:56:31 PM

api/src/main/resources/CalculationRegistration.hbm.xml xml 1.2 KB Dec 13, 2019 12:56:31 PM

api/src/main/resources/liquibase.xml xml 1.5 KB Dec 13, 2019 12:56:31 PM
api/src/main/resources/messages.properties java_properties 3.3 KB Dec 13, 2019 12:56:31 PM
api/src/main/resources/moduleApplicationContext.xml xml 2.4 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/AgeCalculation.java java 30 Lines 4 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/CalculationActivatorTest.java java 20 Lines 2.3 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/CalculationRegistrationValidatorTest.java java 42 Lines 6.8 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/CalculationUtilTest.java java 32 Lines 8.7 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/ClasspathCalculationProviderTest.java java 12 Lines 3.4 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/CountingCalculation.java java 5 Lines 1.8 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/ImplementationConfiguredCalculationProviderTest.java java 11 Lines 1.7 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/InnerCalculation.java java 4 Lines 1.7 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/MostRecentEncounterCalculation.java java 17 Lines 2.9 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/MostRecentObsCalculation.java java 14 Lines 2.6 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/OuterCalculation.java java 9 Lines 1.9 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/RecentEncounterCalculation.java java 20 Lines 3.5 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/api/CalculationRegistrationServiceTest.java java 39 Lines 8 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/patient/PatientBehaviorTest.java java 107 Lines 10.8 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/patient/PatientCalculationServiceTest.java java 41 Lines 7.5 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/result/CalculationResultMapTest.java java 27 Lines 2.7 KB Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/result/ListResultTest.java java 11 Lines Dec 13, 2019 12:56:31 PM
api/src/test/java/org/openmrs/calculation/result/ResultUtilTest.java java 84 Lines 15.7 KB Dec 13, 2019 12:56:31 PM
api/src/test/resources/TestingApplicationContext.xml xml 1.1 KB Dec 13, 2019 12:56:31 PM
api/src/test/resources/org/openmrs/calculation/include/moduleTestData.xml xml 1.9 KB Dec 13, 2019 12:56:31 PM
api/src/test/resources/test-hibernate.cfg.xml xml Dec 13, 2019 12:56:31 PM
api/target/classes/CalculationRegistration.hbm.xml xml 1.2 KB Dec 18, 2019 3:32:50 PM
api/target/classes/liquibase.xml xml 1.5 KB Dec 18, 2019 3:32:50 PM
api/target/classes/messages.properties java_properties 2.7 KB Dec 18, 2019 3:32:50 PM
api/target/classes/moduleApplicationContext.xml xml 2.3 KB Dec 18, 2019 3:32:50 PM
api/target/maven-archiver/pom.properties java_properties Dec 18, 2019 3:32:53 PM
omod/pom.xml xml 6.1 KB Dec 13, 2019 12:56:31 PM
omod/src/main/java/org/openmrs/calculation/web/controller/CalculationAutoRegistrationFormController.java java 47 Lines 5.3 KB Dec 13, 2019 12:56:31 PM
omod/src/main/java/org/openmrs/calculation/web/controller/CalculationRegistrationController.java java 19 Lines 3.8 KB Dec 13, 2019 12:56:31 PM
omod/src/main/java/org/openmrs/calculation/web/controller/CalculationRegistrationFormController.java java 25 Lines 5.7 KB Dec 13, 2019 12:56:31 PM
omod/src/main/java/org/openmrs/calculation/web/extension/AdminList.java java 6 Lines 1.4 KB Dec 13, 2019 12:56:31 PM
omod/src/main/resources/config.xml xml 1.9 KB Dec 13, 2019 12:56:31 PM
omod/src/main/resources/webModuleApplicationContext.xml xml Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/calculationAutoRegistration.jsp jsp 6 Lines 1.7 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/calculationRegistration.jsp jsp 17 Lines 3.1 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/calculationRegistrations.jsp jsp 27 Lines 4 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/localHeader.jsp jsp 2 Lines Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/patientCalculationTest.jsp jsp 19 Lines 3.1 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/resources/dataTables/jquery.dataTables.js typescript 1,184 Lines 116.7 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/resources/dataTables/jquery.dataTables.min.js typescript 440 Lines 52.8 KB Dec 13, 2019 12:56:31 PM
omod/src/main/webapp/resources/jquery-ui/js/jquery-ui-1.7.2.custom.min.js typescript 25 Lines 188.1 KB Dec 13, 2019 12:56:31

PM
omod/target/calculation-1.2/CalculationRegistration.hbm.xml xml 1.2 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/META-INF/maven/org.openmrs.module/calculation-api/pom.properties java_properties Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/META-INF/maven/org.openmrs.module/calculation-api/pom.xml xml 2 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/config.xml xml 1.9 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/liquibase.xml xml 1.5 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/messages.properties java_properties 2.7 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/moduleApplicationContext.xml xml 2.3 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/calculationAutoRegistration.jsp jsp 6 Lines 1.7 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/calculationRegistration.jsp jsp 17 Lines 3.1 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/calculationRegistrations.jsp jsp 27 Lines 4 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/localHeader.jsp jsp 2 Lines Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/patientCalculationTest.jsp jsp 19 Lines 3.1 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/resources/dataTables/jquery.dataTables.js typescript 1,184 Lines 116.7 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/resources/dataTables/jquery.dataTables.min.js typescript 440 Lines 52.8 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/web/module/resources/jquery-ui/js/jquery-ui-1.7.2.custom.min.js typescript 25 Lines 188.1 KB Dec 18, 2019 3:32:56 PM
omod/target/calculation-1.2/webModuleApplicationContext.xml xml Dec 18, 2019 3:32:56 PM
omod/target/classes/CalculationRegistration.hbm.xml xml 1.2 KB Dec 18, 2019 3:32:50 PM
omod/target/classes/META-INF/maven/org.openmrs.module/calculation-api/pom.properties java_properties Dec 18, 2019 3:32:54 PM
omod/target/classes/META-INF/maven/org.openmrs.module/calculation-api/pom.xml xml 2 KB Dec 13, 2019 12:56:32 PM
omod/target/classes/config.xml xml 1.9 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/liquibase.xml xml 1.5 KB Dec 18, 2019 3:32:50 PM
omod/target/classes/messages.properties java_properties 2.7 KB Dec 18, 2019 3:32:50 PM
omod/target/classes/moduleApplicationContext.xml xml 2.3 KB Dec 18, 2019 3:32:50 PM
omod/target/classes/web/module/calculationAutoRegistration.jsp jsp 6 Lines 1.7 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/calculationRegistration.jsp jsp 17 Lines 3.1 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/calculationRegistrations.jsp jsp 27 Lines 4 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/localHeader.jsp jsp 2 Lines Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/patientCalculationTest.jsp jsp 19 Lines 3.1 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/resources/dataTables/jquery.dataTables.js typescript 1,184 Lines 116.7 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/resources/dataTables/jquery.dataTables.min.js typescript 440 Lines 52.8 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/web/module/resources/jquery-ui/js/jquery-ui-1.7.2.custom.min.js typescript 25 Lines 188.1 KB Dec 18, 2019 3:32:55 PM
omod/target/classes/webModuleApplicationContext.xml xml Dec 18, 2019 3:32:55 PM
omod/target/maven-archiver/pom.properties java_properties Dec 18, 2019 3:32:56 PM
pom.xml xml 5.5 KB Dec 13, 2019 12:56:31 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Core, Java
Version: 2019.4.0.0009
ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF
SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, Annotations
Version: 2019.4.0.0009
ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B
SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, JavaScript
Version: 2019.4.0.0009
ID: BD292C4E-4216-4DB8-96C7-9B607BFD9584
SKU: RUL13059

Name: Fortify Secure Coding Rules, Core, Android
Version: 2019.4.0.0009
ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952
SKU: RUL13093

Name: Fortify Secure Coding Rules, Extended, JavaScript
Version: 2019.4.0.0009
ID: C4D1969E-B734-47D3-87D4-73962C1D32E2
SKU: RUL13141

Name: Fortify Secure Coding Rules, Extended, Configuration
Version: 2019.4.0.0009
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Java
Version: 2019.4.0.0009
ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317
SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2019.4.0.0009
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

Name: Fortify Secure Coding Rules, Core, Golang
Version: 2019.4.0.0009
ID: 1DCE79F8-AF6B-474D-A05A-5BFFC8B13DCD
SKU: RUL13218

Name: Fortify Secure Coding Rules, Extended, JSP
Version: 2019.4.0.0009
ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2
SKU: RUL13026

External Metadata:
Version: 2019.4.0.0009

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hiearchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like langauges and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the

"Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA
The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE
The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members

include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007
ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248
The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0

ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].

DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4
ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5

ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930:

CAT II are not considered "In Place".

Name: STIG 4.8
ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.X11.XToolkit
com.fortify.AuthenticationKey=/home/pgupta25/.fortify/config/tools
com.fortify.Core=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core
com.fortify.InstallRoot=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0
com.fortify.InstallationUserName=pgupta25
com.fortify.SCAExecutablePath=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/bin/sourceanalyzer
com.fortify.TotalPhysicalMemory=8363917312
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=/home/pgupta25/.fortify
com.fortify.locale=en
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=calculation
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer
com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settings,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshtml,vbhtml,inc,asp,vbscript,js,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,conf,json,yaml,yml
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/rules
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PH

PLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFileDir=/home/pgupta25/.fortify/sca19.1/log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=/home/pgupta25/.fortify/sca19.1/log/sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshtml,vbhtml
com.fortify.sca.PID=22443
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=/srv/openmrs_code/org/openmrs/module/calculation/calculation_scan.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=PLSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs
com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fi
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler

com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.cpfe.441.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP

com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP
com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4

com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
file.encoding=UTF-8
file.encoding.pkg=sun.io
file.separator=/
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.print.PSPrinterJob
java.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/endorsed
java.ext.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/ext:/usr/java/packages/lib/ext
java.home=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre
java.io.tmpdir=/tmp
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/log4j2.xml
log4j.isThreadContextMapInheritable=true

max.file.path.length=255
os.arch=amd64
os.name=Linux
os.version=4.15.0-58-generic
path.separator=:
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/resources.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/rt.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/sunrsasign.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jsse.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jce.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/charsets.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jfr.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/classes
sun.boot.library.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/amd64
sun.cpu.endian=little
sun.cpu.isalist=
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:SoftRefLRUPolicyMSPerMB=3000 -Dcom.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin -Dcom.fortify.sca.ProjectRoot=/home/pgupta25/.fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=22443 -Xmx4096M -Dcom.fortify.TotalPhysicalMemory=8363917312 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M -Djava.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar -scan @/home/pgupta25/.fortify/Eclipse.Plugin-19.1.0/calculation/calculationScan.txt
sun.jnu.encoding=UTF-8
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=unknown
user.country=US
user.dir=/home/pgupta25
user.home=/home/pgupta25
user.language=en
user.name=pgupta25
user.timezone=America/New_York

Commandline Arguments

-scan
-b
calculation
-format
fpr
-machine-output
-f
/srv/openmrs_code/org/openmrs/module/calculation/calculation_scan.fpr

Warnings

[12002] Could not locate the deployment descriptor (web.xml) for your web application. Please build your web application and try again. File:
/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistrations.jsp
[12003] Assuming Java source level to be 1.8 as it was not specified. Note that the default value may change in future versions.
[12004] The Java frontend was unable to resolve the following include:
/WEB-INF/template/include.jsp at

/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/patientCalculationTest.jsp:1.
/WEB-INF/template/footer.jsp at
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/patientCalculationTest.jsp:86.
/WEB-INF/template/header.jsp at
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/patientCalculationTest.jsp:2.
[12022] The class "javax.servlet.http.HttpServlet" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet-api-3.0.1.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.http.HttpServlet" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[12022] The class "javax.servlet.jsp.PageContext" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet.jsp-api.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.jsp.PageContext" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[1214] Multiple definitions found for class /calculationAutoRegistration.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationAutoRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationAutoRegistration.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationAutoRegistration_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationAutoRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationAutoRegistration.jsp).
[1214] Multiple definitions found for class /calculationRegistration.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationRegistration.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationRegistration_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationRegistration.jsp).
[1214] Multiple definitions found for class /calculationRegistrations.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistrations.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationRegistrations.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationRegistrations_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistrations.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/calculationRegistrations.jsp).
[1214] Multiple definitions found for class /patientCalculationTest.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/patientCalculationTest.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/patientCalculationTest.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientCalculationTest_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/patientCalculationTest.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/calculation-1.2/web/module/patientCalculationTest.jsp).
[1214] Multiple definitions found for class /calculationAutoRegistration.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationAutoRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationAutoRegistration.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationAutoRegistration_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationAutoRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationAutoRegistration.jsp).
[1214] Multiple definitions found for class /calculationRegistration.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationRegistration.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationRegistration_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistration.jsp and
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationRegistration.jsp).
[1214] Multiple definitions found for class /calculationRegistrations.jsp
(/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistrations.jsp and

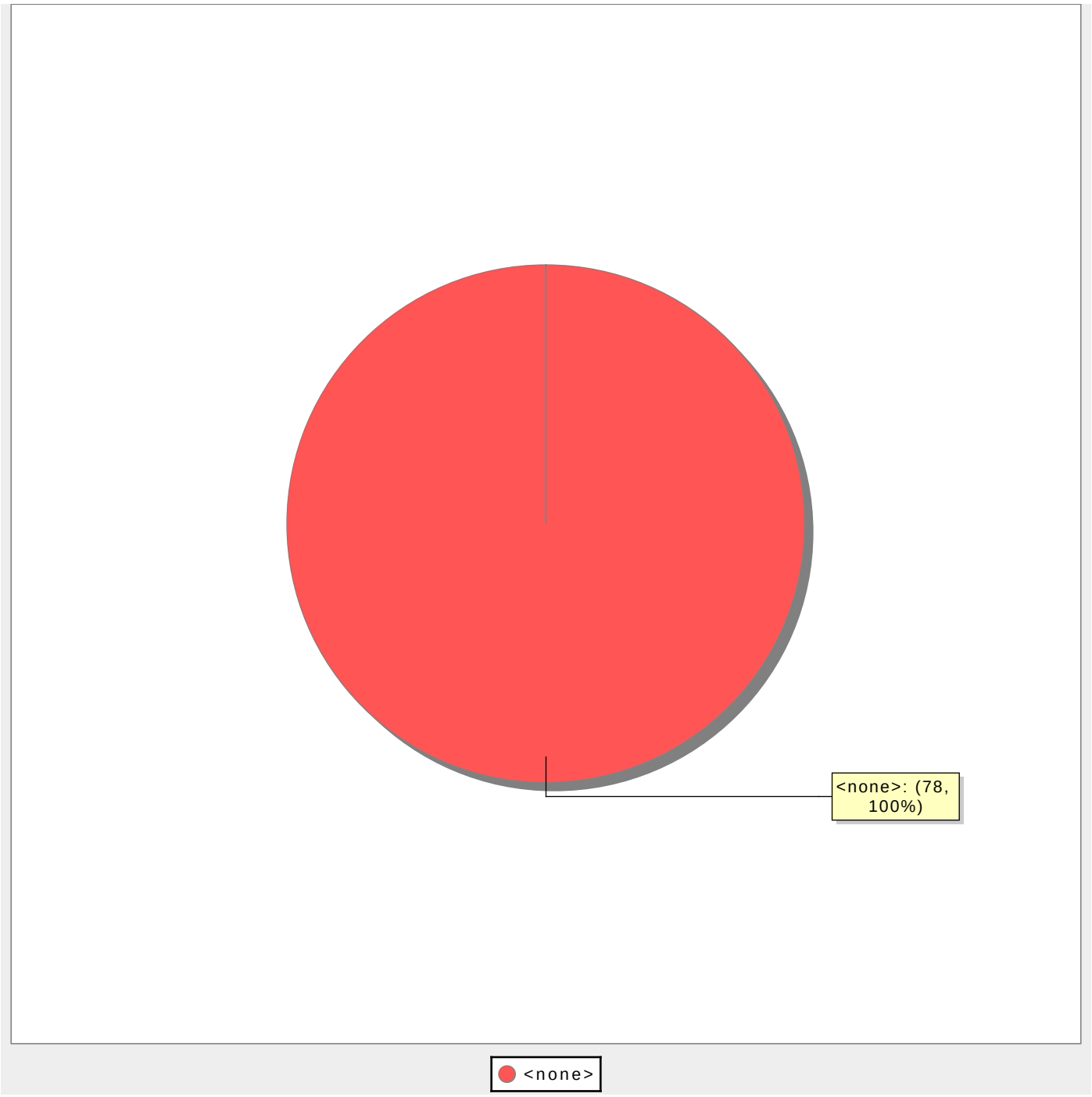
/srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationRegistrations.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculationRegistrations_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/calculationRegistrations.jsp and /srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/calculationRegistrations.jsp).
[1214] Multiple definitions found for class /patientCalculationTest.jsp (/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/patientCalculationTest.jsp and /srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/patientCalculationTest.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientCalculationTest_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/calculation/omod/src/main/webapp/patientCalculationTest.jsp and /srv/openmrs_code/org/openmrs/module/calculation/omod/target/classes/web/module/patientCalculationTest.jsp).
[1215] Could not locate the root (WEB-INF) of the web application. Please build your web application and try again.

Issue Count by Category

Issues by Category	
Cross-Site Scripting: DOM	66
Dynamic Code Evaluation: Code Injection	6
Header Manipulation: Cookies	6

Issue Breakdown by Analysis

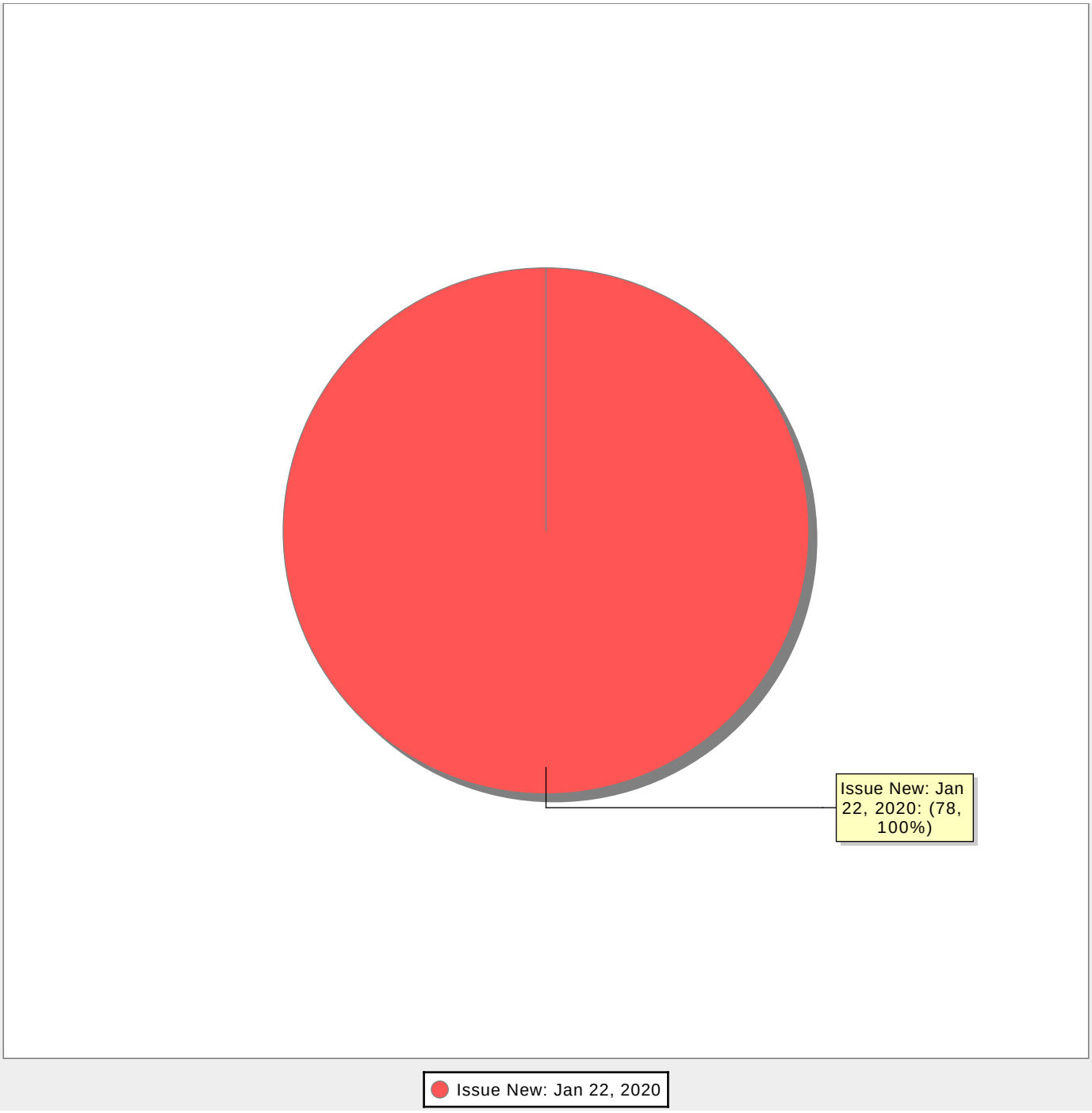
Issues by Analysis



New Issues

Issues by New Issue

The following issues have been discovered since the last scan.



Fortify Security Report

Jan 28, 2020

pgupta25

Executive Summary

Issues Overview

On Jan 28, 2020, a source code review was performed over the reportingcompatibility code base. 482 files, 11,574 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 40 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
High	23
Critical	17

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: /srv/openmrs_code/org/openmrs/module/reportingcompatibility
Number of Files: 482
Lines of Code: 11574
Build Label: <No Build Label>

Scan Information

Scan time: 13:56
SCA Engine version: 19.1.0.2241
Machine Name: vclv99-89.hpc.ncsu.edu
Username running scan: pgupta25

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
File System:
java.io.FileInputStream.FileInputStream
java.io.FileInputStream.FileInputStream

Private Information:
java.util.Properties.getProperty

System Information:
null.null.null
java.lang.Throwable.getMessage

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical

If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
If impact is not in range [2.5, 5.0] Then hide issue
If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

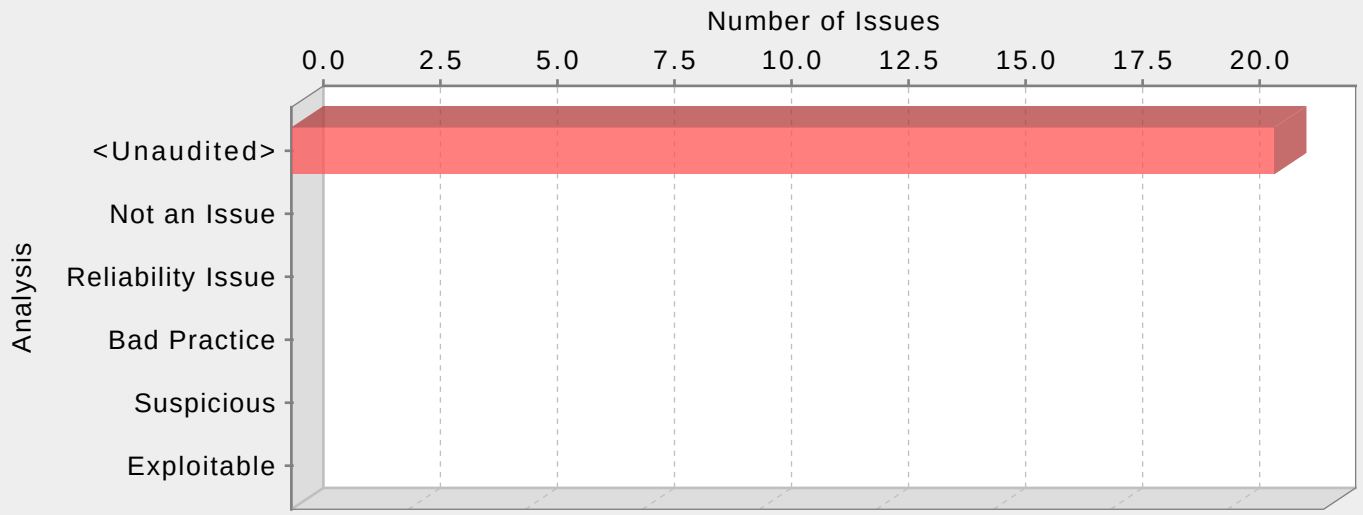
Results Outline

Overall number of results

The scan found 40 issues.

Vulnerability Examples by Category

Category: Log Forging (21 Issues)



Abstract:

The method createCompositionFilter() in CohortSearchHistory.java writes unvalidated user input to the log on line 404. An attacker could take advantage of this behavior to forge log entries or inject malicious content into the log.

Explanation:

Log forging vulnerabilities occur when:

1. Data enters an application from an untrusted source.

2. The data is written to an application or system log file.

Applications typically use log files to store a history of events or transactions for later review, statistics gathering, or debugging. Depending on the nature of the application, the task of reviewing log files may be performed manually on an as-needed basis or automated with a tool that automatically culls logs for important events or trending information.

Interpretation of the log files may be hindered or misdirected if an attacker can supply data to the application that is subsequently logged verbatim. In the most benign case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker may be able to render the file unusable by corrupting the format of the file or injecting unexpected characters. A more subtle attack might involve skewing the log file statistics. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to implicate another party in the commission of a malicious act [1]. In the worst case, an attacker may inject code or other commands into the log file and take advantage of a vulnerability in the log processing utility [2].

Example 1: The following web application code attempts to read an integer value from a request object. If the value fails to parse as an integer, then the input is logged with an error message indicating what happened.

```
...
String val = request.getParameter("val");
try {
int value = Integer.parseInt(val);
}
catch (NumberFormatException nfe) {
log.info("Failed to parse val = " + val);
}
...
```

If a user submits the string "twenty-one" for val, the following entry is logged:

```
INFO: Failed to parse val=twenty-one
```

However, if an attacker submits the string "twenty-one%0a%0aINFO:+User+logged+out%3dbadguy", the following entry is logged:

INFO: Failed to parse val=twenty-one

INFO: User logged out=badguy

Clearly, attackers may use this same mechanism to insert arbitrary log entries.

Some think that in the mobile world, classic web application vulnerabilities, such as log forging, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 2: The following code adapts Example 1 to the Android platform.

```
...
String val = this.getIntent().getExtras().getString("val");
try {
int value = Integer.parseInt();
}
catch (NumberFormatException nfe) {
Log.e(TAG, "Failed to parse val = " + val);
}
...
```

Recommendations:

Prevent log forging attacks with indirection: create a set of legitimate log entries that correspond to different events that must be logged and only log entries from this set. To capture dynamic content, such as users logging out of the system, always use server-controlled values rather than user-supplied data. This ensures that the input provided by the user is never used directly in a log entry.

Example 1 can be rewritten to use a pre-defined log entry that corresponds to a NumberFormatException as follows:

```
...
public static final String NFE = "Failed to parse val. The input is required to be an integer value."
...
String val = request.getParameter("val");
try {
int value = Integer.parseInt(val);
}
catch (NumberFormatException nfe) {
log.info(NFE);
}
..
```

And here is an Android equivalent:

```
...
public static final String NFE = "Failed to parse val. The input is required to be an integer value."
...
String val = this.getIntent().getExtras().getString("val");
try {
int value = Integer.parseInt();
}
catch (NumberFormatException nfe) {
Log.e(TAG, NFE);
}
...
```

In some situations this approach is impractical because the set of legitimate log entries is too large or complicated. In these situations, developers often fall back on blacklisting. Blacklisting selectively rejects or escapes potentially dangerous characters before using the input. However, a list of unsafe characters can quickly become incomplete or outdated. A better approach is to create a whitelist of characters that are allowed to appear in log entries and accept input composed exclusively of characters in the approved set. The most critical character in most log forging attacks is the '\n' (newline) character, which should never appear on a log entry whitelist.

Tips:

1. Many logging operations are created only for the purpose of debugging a program during development and testing. In our experience, debugging will be enabled, either accidentally or purposefully, in production at some point. Do not excuse log forging vulnerabilities simply because a programmer says "I don't have any plans to turn that on in production".

2. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, the Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

CohortSearchHistory.java, line 404 (Log Forging)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method createCompositionFilter() in CohortSearchHistory.java writes unvalidated user input to the log on line 404. An attacker could take advantage of this behavior to forge log entries or inject malicious content into the log.		

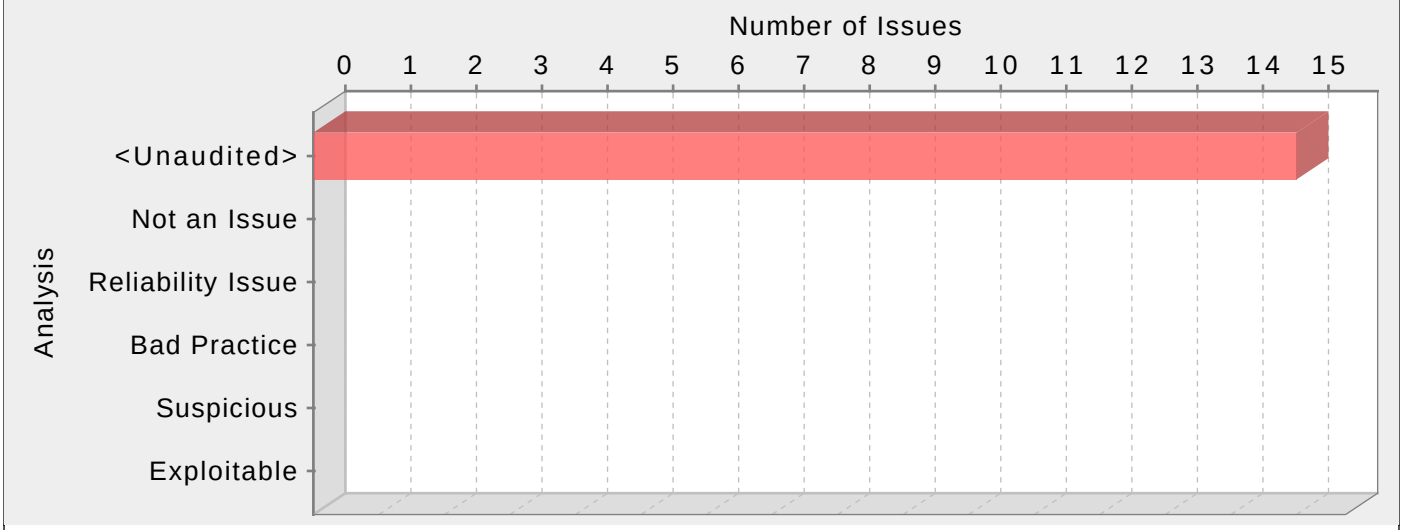
Source: CohortBuilderController.java:403 javax.servlet.ServletRequest.getParameter()

```
401                 log.warn("addCohort(id) didn't find " + cohortId);
402               }
403               temp = request.getParameter("composition");
404               if (temp != null) {
405                PatientSearch ps = history.createCompositionFilter(temp);
```

Sink: CohortSearchHistory.java:404 org.apache.commons.logging.Log.error()

```
402               }
403               catch (Exception ex) {
404                log.error("Error in description string: " + description, ex);
405                return null;
406               }
```

Category: Cross-Site Scripting: Reflected (15 Issues)



Abstract:

The method _jspService() in cohortReportForm.jsp sends unvalidated data to a web browser on line 61, which can result in the browser executing malicious code.

Explanation:

Cross-site scripting (XSS) vulnerabilities occur when:

1. Data enters a web application through an untrusted source. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store.

2. The data is included in dynamic content that is sent to a web user without being validated.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Example 1: The following JSP code segment reads an employee ID, eid, from an HTTP request and displays it to the user.

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The code in this example operates correctly if eid contains only standard alphanumeric text. If eid has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL which causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS.

Example 2: The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

```
<%...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
}
%>
Employee Name: <%= name %>
```

As in Example 1, this code functions correctly when the values of name are well-behaved, but it does nothing to prevent exploits if they are not. Again, this code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker may execute malicious commands in the user's web browser. This type of exploit, known as Persistent (or Stored) XSS, is particularly insidious because the indirection caused by the data store makes it more difficult to identify the threat and increases the possibility that the attack will affect multiple users. XSS got its start in this form with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code.

Some think that in the mobile world, classic web application vulnerabilities, such as cross-site scripting, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 3: The following code enables JavaScript in Android's WebView (by default, JavaScript is disabled) and loads a page based on the value received from an Android intent.

```
...
WebView webview = (WebView) findViewById(R.id.webview);
webview.getSettings().setJavaScriptEnabled(true);
String url = this.getIntent().getExtras().getString("url");
webview.loadUrl(url);
...
```

If the value of url starts with javascript:, JavaScript code that follows will execute within the context of the web page inside WebView.

As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim:

- As in Example 1, data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities.

- As in Example 2, the application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

- As in Example 3, a source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, the rulepacks dynamically re-prioritize the issues reported by Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

Recommendations:

The solution to XSS is to ensure that validation occurs in the correct places and checks are made for the correct properties.

Since XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application may accept input through a shared data store or other trusted source, and that data store may accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user.

The most secure approach to validation for XSS is to create a whitelist of safe characters that are allowed to appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alpha-numeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser should still be considered valid input once they are encoded, such as a web design bulletin board that must accept HTML fragments from its users.

A more flexible, but less secure approach is known as blacklisting, which selectively rejects or escapes potentially dangerous characters before using the input. In order to form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines what characters have special meaning, many web browsers try to correct common mistakes in HTML and may treat other characters as special in certain contexts, which is why we do not encourage the use of blacklists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]:

In the content of a block-level element (in the middle of a paragraph of text):

- "<" is special because it introduces a tag.

- "&" is special because it introduces a character entity.

- ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error.

The following principles apply to attribute values:

- In attribute values enclosed with double quotes, the double quotes are special because they mark the end of the attribute value.

- In attribute values enclosed with single quote, the single quotes are special because they mark the end of the attribute value.

- In attribute values without any quotes, white-space characters, such as space and tab, are special.

- "&" is special when used with certain attributes, because it introduces a character entity.

In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters:

- Space, tab, and new line are special because they mark the end of the URL.

- "&" is special because it either introduces a character entity or separates CGI parameters.

- Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context.

- The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server -side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page in question.

Within the body of a <SCRIPT> </SCRIPT>:

- Semicolons, parentheses, curly braces, and new line characters should be filtered out in situations where text could be inserted directly into a pre-existing script tag.

Server-side scripts:

- Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering.

Other possibilities:

- If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and may bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7).

After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option in this situation is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and may be unacceptable in circumstances where the integrity of the input must be preserved for display.

If input containing special characters must be accepted and displayed accurately, validation must encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2].

Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. When an application is developed there are no guarantees about what application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will also stay in sync.

Tips:

1. The Fortify Secure Coding Rulepacks warn about SQL Injection and Access Control: Database issues when untrusted data is written to a database and also treat the database as a source of untrusted data, which can lead to XSS vulnerabilities. If the database is a trusted resource in your environment, use custom filters to filter out dataflow issues that include the DATABASE taint flag or originate from database sources. Nonetheless, it is often still a good idea to validate everything read from the database.

2. Even though URL encoding untrusted data protects against many XSS attacks, some browsers (specifically, Internet Explorer 6 and 7 and possibly others) automatically decode content at certain locations within the Document Object Model (DOM) prior to passing it to the JavaScript interpreter. To reflect this danger, the rulepacks no longer treat URL encoding routines as sufficient to protect against cross-site scripting. Data values that are URL encoded and subsequently output will cause Fortify to report Cross-Site Scripting: Poor Validation vulnerabilities.

3. Fortify RTA adds protection against this category.

cohortReportForm.jsp, line 61 (Cross-Site Scripting: Reflected)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The method _jspService() in cohortReportForm.jsp sends unvalidated data to a web browser on line 61, which can result in the browser executing malicious code.		

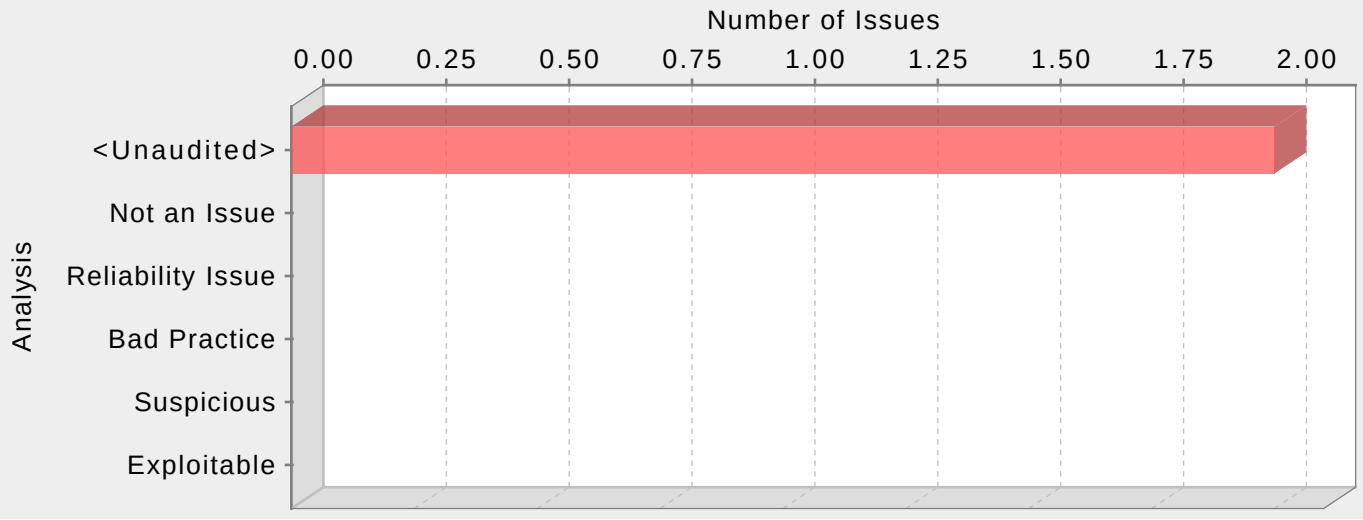
Source: cohortReportForm.jsp:61 javax.servlet.ServletRequest.getParameter()

```
59    <c:forEach var="clazz" items="${parameterClasses}">
60     opt = document.createElement("option");
61     <c:if test="${param.clazz == clazz}">
62      opt.setAttribute("selected", "true");
63     </c:if>
```

Sink: cohortReportForm.jsp:61 javax.servlet.jsp.JspWriter.print()

```
59    <c:forEach var="clazz" items="${parameterClasses}">
60     opt = document.createElement("option");
61     <c:if test="${param.clazz == clazz}">
62      opt.setAttribute("selected", "true");
63     </c:if>
```

Category: Denial of Service: Regular Expression (2 Issues)



Abstract:

Untrusted data is passed to the application and used as a regular expression. This can cause the thread to overconsume CPU resources.

Explanation:

There is a vulnerability in implementations of regular expression evaluators and related methods that can cause the thread to hang when evaluating regular expressions that contain a grouping expression that is itself repeated. Additionally, any regular expression that contains alternate subexpressions that overlap one another can also be exploited. This defect can be used to execute a Denial of Service (DoS) attack.

Example:

(e+)+

([a-zA-Z]+)*

(e|ee)+

There are no known regular expression implementations which are immune to this vulnerability. All platforms and languages are vulnerable to this attack.

Recommendations:

Do not allow untrusted data to be used as regular expression patterns.

EvaluationContext.java, line 354 (Denial of Service: Regular Expression)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	Untrusted data is passed to the application and used as a regular expression. This can cause the thread to overconsume CPU resources.		

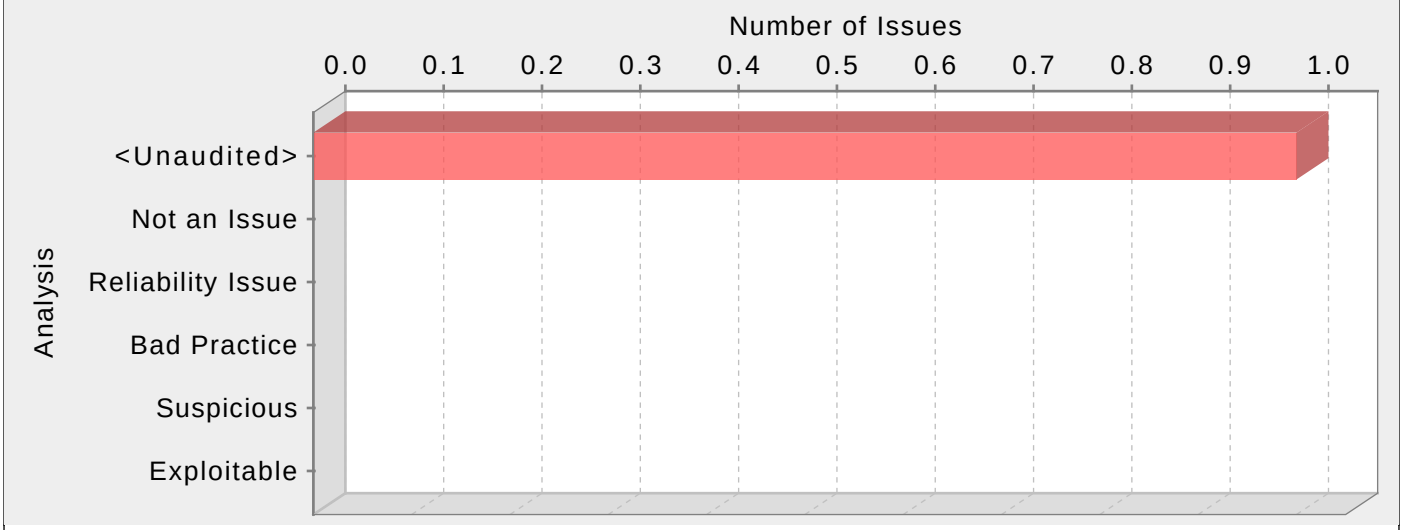
Source: CohortBuilderController.java:523 javax.servlet.ServletRequest.getParameter()

```
521      }
522      argValues
523              .add(new ArgHolder(c, name, isList ? request.getParameterValues(name) :
request.getParameter(name)));
524    }
525
```

Sink: EvaluationContext.java:354 java.lang.String.replaceAll()

```
352           log.debug("Calculated date of: " + foundDate);
353         }
354         replacement = replacement.replaceAll("\\Q" + m.group(0) + "\\E", foundDate);
355         log.debug("Modified to: " + replacement);
356       }
```

Category: Dynamic Code Evaluation: XMLDecoder Injection (1 Issues)



Abstract:

The file ReportObjectXMLDecoder.java deserializes unvalidated XML input using java.beans.XMLDecoder on line 33. Deserializing user-controlled XML documents at run-time can allow attackers to execute malicious arbitrary code on the server.

Explanation:

The JDK XMLEncoder and XMLDecoder classes provide the developer with an easy way to persist objects, serializing them to XML documents. But XMLEncoder also allows a developer to serialize method calls and if an attacker can provide the XML document to be deserialized by XMLDecoder, he may be able to execute any arbitrary code on the server.

Example: The following Java code shows an instance of XMLDecoder processing untrusted input.

```
XMLDecoder decoder = new XMLDecoder(new InputSource(new InputStreamReader(request.getInputStream(), "UTF-8")));
Object object = decoder.readObject();
decoder.close();
```

Example: The following XML document will instantiate a ProcessBuilder object and will invoke its static start() method to run the windows calculator.

```
<java>
<object class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="1" >
<void index="0">
<string>c:\\windows\\system32\\calc.exe</string>
</void>
</array>
<void method="start"/>
</object>
</java>
```

Recommendations:

Unfortunately there is no way to avoid code execution during the XMLDecoder deserialization process. Never use XMLDecoder with user-controlled data, but if there is no alternative, run a strong validation routine to avoid malicious payloads.

Tips:

1. Please disregard this issue if it was found in a Restlet 2.1.4 or later application.

ReportObjectXMLDecoder.java, line 33 (Dynamic Code Evaluation: XMLDecoder Injection)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file ReportObjectXMLDecoder.java deserializes unvalidated XML input using java.beans.XMLDecoder on line 33. Deserializing user-controlled XML documents at run-time can allow attackers to execute malicious arbitrary code on the server.		
Source:	PatientSearchFormController.java:75 javax.servlet.ServletRequest.getParameter()		

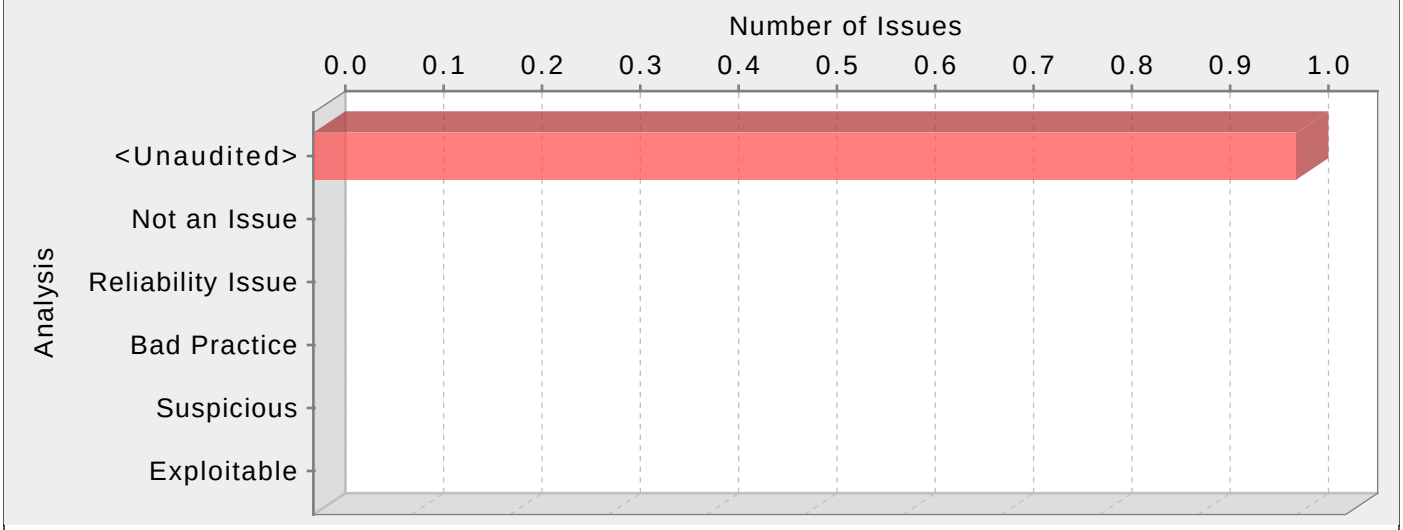
```
73          int hasXMLChanged = 0;
```

```
74                      hasXMLChanged = Integer.parseInt(request.getParameter("patientSearchXMLHasChanged"));
75                      String textAreaXML = request.getParameter("xmlStringTextArea");
76                      Integer argumentsLength = Integer.valueOf(request.getParameter("argumentsSize"));
77                      PatientSearch ps = null;
```

Sink: ReportObjectXMLDecoder.java:33 java.beans.XMLDecoder.XMLDecoder()

```
31                   public AbstractReportObject toAbstractReportObject() {
32                    ExceptionListener exListener = new ReportObjectWrapperExceptionListener();
33                    XMLDecoder dec = new XMLDecoder(new BufferedInputStream(new
                    ByteArrayInputStream(xmlToDecode.getBytes())), null,
34                            exListener);
35                    AbstractReportObject o = (AbstractReportObject) dec.readObject();
```

Category: XML External Entity Injection (1 Issues)



Abstract:

XML parser configured in ReportObjectXMLDecoder.java:33 does not prevent nor limit external entities resolution. This can expose the parser to an XML External Entities attack.

Explanation:

XML External Entities attacks benefit from an XML feature to build documents dynamically at the time of processing. An XML entity allows inclusion of data dynamically from a given resource. External entities allow an XML document to include data from an external URI. Unless configured to do otherwise, external entities force the XML parser to access the resource specified by the URI, e.g., a file on the local machine or on a remote system. This behavior exposes the application to XML External Entity (XXE) attacks, which can be used to perform denial of service of the local system, gain unauthorized access to files on the local machine, scan remote machines, and perform denial of service of remote systems.

The following XML document shows an example of an XXE attack.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///dev/random" >]><foo>&xxe;</foo>
```

This example could crash the server (on a UNIX system), if the XML parser attempts to substitute the entity with the contents of the /dev/random file.

Recommendations:

The XML unmarshaller should be configured securely so that it does not allow external entities as part of an incoming XML document.

To avoid XXE injection do not use unmarshal methods that process an XML source directly as java.io.File, java.io.Reader or java.io.InputStream. Parse the document with a securely configured parser and use an unmarshal method that takes the secure parser as the XML source as shown in the following example:

```
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
dbf.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true);
DocumentBuilder db = dbf.newDocumentBuilder();
Document document = db.parse(<XML Source>);
Model model = (Model) u.unmarshal(document);
```

Tips:

1. Fortify RTA adds protection against this category.

ReportObjectXMLDecoder.java, line 33 (XML External Entity Injection)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	XML parser configured in ReportObjectXMLDecoder.java:33 does not prevent nor limit external entities resolution. This can expose the parser to an XML External Entities attack.		
Source:	PatientSearchFormController.java:75 javax.servlet.ServletRequest.getParameter()		

```
73              int hasXMLChanged = 0;
```

```
74                      hasXMLChanged = Integer.parseInt(request.getParameter("patientSearchXMLHasChanged"));
75                      String textAreaXML = request.getParameter("xmlStringTextArea");
76                      Integer argumentsLength = Integer.valueOf(request.getParameter("argumentsSize"));
77                      PatientSearch ps = null;
```

Sink: ReportObjectXMLDecoder.java:33 java.beans.XMLDecoder.XMLDecoder()

```
31                   public AbstractReportObject toAbstractReportObject() {
32                    ExceptionListener exListener = new ReportObjectWrapperExceptionListener();
33                    XMLDecoder dec = new XMLDecoder(new BufferedInputStream(new
                    ByteArrayInputStream(xmlToDecode.getBytes())), null,
34                              exListener);
35                    AbstractReportObject o = (AbstractReportObject) dec.readObject();
```

Detailed Project Summary

Files Scanned

Code base location: /srv/openmrs_code/org/openmrs/module/reportingcompatibility
Files Scanned:
.travis.yml yaml Dec 13, 2019 12:57:03 PM
/home/pgupta25/.fortify/sca19.1/build/reportingcompatibility/extracted/javascript/srv/openmrs_code/org/openmrs/module/reportingcompatibility/api/src/main/java/org/openmrs/cohort/package.html.js secondary Jan 28, 2020 11:25:16 PM
/home/pgupta25/.fortify/sca19.1/build/reportingcompatibility/extracted/javascript/srv/openmrs_code/org/openmrs/module/reportingcompatibility/api/src/main/java/org/openmrs/report/package.html.js secondary Jan 28, 2020 11:25:16 PM
/home/pgupta25/.fortify/sca19.1/build/reportingcompatibility/extracted/javascript/srv/openmrs_code/org/openmrs/module/reportingcompatibility/api/src/main/java/org/openmrs/reporting/package.html.js secondary Jan 28, 2020 11:25:15 PM
api/pom.xml xml 3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/Cohort.java java 66 Lines 7.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/CohortDefinition.java java 1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/CohortDefinitionItemHolder.java java 15 Lines 2.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/CohortDefinitionProvider.java java 3.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/CohortSearchHistory.java java 186 Lines 13.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/CohortUtil.java java 50 Lines 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/StaticCohortDefinition.java java 8 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/impl/PatientSearchCohortDefinitionProvider.java java 20 Lines 4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/impl/StaticCohortDefinitionProvider.java java 20 Lines 4.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/cohort/package.html html Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/CohortBuilderLinkProvider.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/ModuleActivator.java java 4 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/ReportingCompatibilityConstants.java java 5 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/extension/html/AdminList.java java 19 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/extension/html/CohortBuilderHeader.java java 5 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/reporting/SqlPatientFilter.java java 21 Lines 2.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/reporting/export/DataExportFunctions.java java 382 Lines 43.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/reporting/export/DataExportUtil.java java 69 Lines 10 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/CohortService.java java 4.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/CohortServiceImpl.java java 40 Lines 7.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/DataSetService.java java 2.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/ReportService.java java 8 Lines 24.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/ReportingCompatibilityService.java java 24.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/ReportingCompatibilityServiceImpl.java java 134 Lines 22.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/db/HibernateReportingCompatibilityDAO.java java 792 Lines 75.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/module/reportingcompatibility/service/db/ReportingCompatibilityDAO.java java 9.1 KB Dec 13,

2019 12:57:03 PM
api/src/main/java/org/openmrs/propertyeditor/AbstractReportObjectEditor.java java 16 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/propertyeditor/DataExportReportObjectEditor.java java 16 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/propertyeditor/ReportDefinitionEditor.java java 16 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/propertyeditor/ReportSchemaXmlEditor.java java 12 Lines 1.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/CohortDataSet.java java 12 Lines 2.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/CohortDataSetDefinition.java java 26 Lines 5.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/CohortDataSetProvider.java java 16 Lines 2.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/DataSet.java java 2.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/DataSetDefinition.java java 2.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/DataSetProvider.java java 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/DataSetTransform.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/EvaluationContext.java java 102 Lines 13.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/MapDataSet.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/Parameter.java java 16 Lines 3.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ParameterException.java java 3 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/Parameterizable.java java 1.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RenderingException.java java 2 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RenderingMode.java java 17 Lines 2.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportConstants.java java 14 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportData.java java 7 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportDesigner.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportRenderer.java java 3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportRenderingException.java java 2 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportSchema.java java 21 Lines 5.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/ReportSchemaXml.java java 26 Lines 4.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerObsDataSet.java java 24 Lines 3.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerObsDataSetDefinition.java java 34 Lines 4.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerObsDataSetProvider.java java 18 Lines 2.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerProgramEnrollmentDataSet.java java 21 Lines 2.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerProgramEnrollmentDataSetDefinition.java java 26 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/RowPerProgramEnrollmentDataSetProvider.java java 15 Lines 2.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/db/ReportDAO.java java 6.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/db/hibernate/HibernateReportDAO.java java 522 Lines 51.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/impl/CsvReportRenderer.java java 10 Lines 1.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/impl/DataSetServiceImpl.java java 18 Lines 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/impl/DelimitedTextReportRenderer.java java 27 Lines 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/impl/ReportServiceImpl.java java 181 Lines 28.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/impl/TsvReportRenderer.java java 11 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/report/package.html html Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/AbstractPatientDataProducer.java java 4 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/AbstractPatientFilter.java java 15 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/AbstractReportObject.java java 22 Lines 3.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CachingPatientFilter.java java 16 Lines 3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CohortFilter.java java 13 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CohortHistoryCompositionFilter.java java 44 Lines 5.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CompoundClassifier.java java 10 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CompoundPatientFilter.java java 38 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/CountAggregator.java java 2 Lines Dec 13, 2019 12:57:03 PM

api/src/main/java/org/openmrs/reporting/DataTable.java java 55 Lines 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/DateColumnClassifier.java java 10 Lines 1.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/DrugOrderFilter.java java 86 Lines 8.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/DrugOrderPatientFilter.java java 42 Lines 4.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/DrugOrderPatientFilterValidator.java java 2 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/DrugOrderStopFilter.java java 88 Lines 8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/EmptyReportObject.java java 1 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/EncounterPatientFilter.java java 68 Lines 7.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/InversePatientFilter.java java 13 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/LocationPatientFilter.java java 19 Lines 2.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/LogicPatientFilter.java java 22 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/NumericRangeColumnClassifier.java java 32 Lines 2.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ObsPatientFilter.java java 95 Lines 8.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PatientCharacteristicFilter.java java 94 Lines 8.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PatientCharacteristicFilterValidator.java java 2 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PatientFilter.java java 1.8 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PatientSearch.java java 188 Lines 19.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PatientSearchReportObject.java java 8 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/PersonAttributeFilter.java java 19 Lines 2.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ProgramPatientFilter.java java 31 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ProgramStatePatientFilter.java java 78 Lines 7.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/RelationshipPatientFilter.java java 34 Lines 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/Report.java java 23 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObject.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectFactory.java java 95 Lines 9.4 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectFactoryModule.java java 11 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectList.java java 8 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectService.java java 7.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectWrapper.java java 54 Lines 6.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectWrapperExceptionListener.java java 3 Lines 1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectXMLDecoder.java java 9 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/ReportObjectXMLEncoder.java java 119 Lines 13.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/SearchArgument.java java 12 Lines 1.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/SimpleColumnClassifier.java java 5 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/TableGroupAndAggregate.java java 18 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/TableRow.java java 5 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/TableRowAggregator.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/TableRowClassifier.java java Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/data/CohortDefinition.java java 8 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/data/DatasetDefinition.java java 12 Lines 2.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/db/ReportObjectDAO.java java 1.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/db/hibernate/HibernateReportObjectDAO.java java 45 Lines 6.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/CalculatedColumn.java java 5 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/CohortColumn.java java 37 Lines 4.2 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/ConceptColumn.java java 107 Lines 9.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/DataExportFunctions.java java 354 Lines 38.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/DataExportReportObject.java java 73 Lines 8.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/DataExportUtil.java java 62 Lines 9.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/ExportColumn.java java 2 Lines Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/RowPerObsColumn.java java 40 Lines 4 KB Dec 13, 2019 12:57:03 PM

api/src/main/java/org/openmrs/reporting/export/RowPerObsDataExportReportObject.java java 77 Lines 9.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/export/SimpleColumn.java java 16 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/impl/ReportObjectServiceImpl.java java 57 Lines 11.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/package.html html Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/report/ReportDefinition.java java 25 Lines 5.1 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/reporting/report/ReportElementDefinition.java java 8 Lines 1.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/scheduler/tasks/GenerateDataExportTask.java java 20 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/util/ReportingcompatibilityUtil.java java 115 Lines 11.5 KB Dec 13, 2019 12:57:03 PM
api/src/main/java/org/openmrs/validator/ReportObjectValidator.java java 3 Lines 2.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/resources/ReportObject.hbm.xml xml 2.3 KB Dec 13, 2019 12:57:03 PM
api/src/main/resources/ReportSchemaXml.hbm.xml xml 1.1 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/cohort/CohortUtilTest.java java 15 Lines 3.3 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/module/reportingcompatibility/service/CohortServiceTest.java java 8 Lines 2.4 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/EvaluationContextTest.java java 22 Lines 3.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/PatientSearchParameterTest.java java 38 Lines 5.5 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/PatientSearchTest.java java 30 Lines 4.5 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/PepfarReportFromXmlTest.java java 102 Lines 11.1 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/PepfarReportSerializationTest.java java 39 Lines 8.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/PepfarReportTest.java java 58 Lines 7.7 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/ReportSchemaXmlNonContextTest.java java 145 Lines 10.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/ReportSchemaXmlTest.java java 126 Lines 11 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/RowPerObsDatasetTest.java java 25 Lines 4.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/report/RowPerProgramEnrollmentDatasetTest.java java 16 Lines 3 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/CachingPatientFilterTest.java java 14 Lines 2 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/InversePatientFilterTest.java java 42 Lines 5.8 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/PatientFilterTest.java java 22 Lines 2.5 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/ReportObjectServiceTest.java java 14 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/export/DataExportTest.java java 276 Lines 22.9 KB Dec 13, 2019 12:57:03 PM
api/src/test/java/org/openmrs/reporting/export/RowPerObsDataExportTest.java java 25 Lines 4.4 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/TestingApplicationContext.xml xml 7.1 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/PatientSearchParameterTest.xml xml 9.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/PatientSearchTest.xml xml 3.8 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/PepfarReportTest.xml xml 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/ReportSchemaXmlTest-initialData.xml xml 10.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/ReportTests-obs.xml xml 11 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/ReportTests-patients.xml xml 7.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/RowPerObsDatasetTest.xml xml 3.9 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/report/include/RowPerProgramEnrollment.xml xml 1.6 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/reporting/export/include/DataExportTest-obs.xml xml 10.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/reporting/export/include/DataExportTest-patients.xml xml 1.2 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/org/openmrs/reporting/include/PatientFilterTest.xml xml 2.5 KB Dec 13, 2019 12:57:03 PM
api/src/test/resources/test-hibernate.cfg.xml xml Dec 13, 2019 12:57:03 PM
api/target/classes/ReportObject.hbm.xml xml 2.3 KB Dec 18, 2019 11:54:23 AM
api/target/classes/ReportSchemaXml.hbm.xml xml 1.1 KB Dec 18, 2019 11:54:23 AM
api/target/maven-archiver/pom.properties java_properties Dec 18, 2019 11:55:41 AM
omod/pom.xml xml 4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/PatientSetPortletController.java java 29 Lines 3.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/analysis/CohortBuilderController.java java 238 Lines 20.6 KB Dec 13, 2019 12:57:03 PM

omod/src/main/java/org/openmrs/web/controller/report/CohortListController.java java 36 Lines 5.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/CohortReportFormController.java java 244 Lines 19.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/PatientSearchFormController.java java 91 Lines 8.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/PatientSearchListController.java java 50 Lines 6.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportDataFormController.java java 51 Lines 6.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportDataListController.java java 24 Lines 4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportMacrosFormController.java java 13 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportObjectFormController.java java 95 Lines 12.7 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportObjectListController.java java 33 Lines 5.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportObjectValidator.java java 1 Lines Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportSchemaXmlFormController.java java 53 Lines 6.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportSchemaXmlListController.java java 3 Lines 1.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportValidator.java java 4 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/ReportsListController.java java 3 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/RunReportController.java java 62 Lines 7.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/export/DataExportFormController.java java 83 Lines 10.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/export/DataExportListController.java java 77 Lines 10.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/export/RowPerObsDataExportFormController.java java 74 Lines 9.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/controller/report/export/RowPerObsDataExportListController.java java 64 Lines 8.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/dwr/DWRCohortBuilderService.java java 108 Lines 11.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/dwr/DWRPatientSetService.java java 12 Lines 1.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/report/CohortReportWebRenderer.java java 9 Lines 3.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/report/WebReportRenderer.java java 1.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/servlet/DataExportServlet.java java 28 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/java/org/openmrs/web/taglib/ForEachReportObjectTag.java java 33 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/config.xml xml 4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages.properties java_properties 24.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages_en_GB.properties java_properties Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages_es.properties java_properties 14.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages_fr.properties java_properties 1.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages_it.properties java_properties 13.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/messages_pt.properties java_properties 2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/moduleApplicationContext.xml xml 17.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/resources/sqldiff.xml xml Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/analysis/cohortBuilder.jsp jsp 110 Lines 63.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/portlets/patientSet.jsp jsp 34 Lines 8.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/cohortList.jsp jsp 15 Lines 1.8 KB Dec 13, 2019 12:57:03 PM

omod/src/main/webapp/reports/cohortReportForm.jsp jsp 44 Lines 14.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/dataExportForm.jsp jsp 48 Lines 28.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/dataExportList.jsp jsp 14 Lines 3.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/include/calculatedColumns.jsp jsp 1 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/include/cohortColumns.jsp jsp 6 Lines 1.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/include/conceptColumns.jsp jsp 1 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/include/simpleColumns.jsp jsp 26 Lines 9.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/localHeader.jsp jsp 19 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/patientSearchForm.jsp jsp 17 Lines 4.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/patientSearchList.jsp jsp 6 Lines 1.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportDataForm.jsp jsp 27 Lines 4.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportDataList.jsp jsp 11 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportMacrosForm.jsp jsp 3 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportObjectForm.jsp jsp 34 Lines 5.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportObjectList.jsp jsp 11 Lines 1.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportSchemaXmlForm.jsp jsp 6 Lines 1.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/reportSchemaXmlList.jsp jsp 6 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/rowPerObsDataExportForm.jsp jsp 46 Lines 28.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/rowPerObsDataExportList.jsp jsp 9 Lines 2.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/runReportForm.jsp jsp 23 Lines 2.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/reports/runReportList.jsp jsp 5 Lines 1.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-am.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ar.js typescript 27 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-bg.js typescript 17 Lines 1.7 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ca.js typescript 17 Lines 1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-cs.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-da.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-de.js typescript 17 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-es.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fi.js typescript 18 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fr.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-he.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-hu.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-id.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-is.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-it.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM

omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ja.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ko.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lt.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lv.js typescript 18 Lines 1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-nl.js typescript 17 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-no.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pl.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pt-BR.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ro.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ru.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sk.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sv.js typescript 17 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-th.js typescript 17 Lines 1.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-tr.js typescript 17 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ua.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-CN.js typescript 17 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-TW.js typescript 18 Lines 1.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.blind.packed.js typescript 1 Lines Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.bounce.packed.js typescript 1 Lines 1.5 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.clip.packed.js typescript 1 Lines 1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.core.packed.js typescript 1 Lines 8.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.drop.packed.js typescript 1 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.explode.packed.js typescript 1 Lines 1.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.fold.packed.js typescript 1 Lines Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.highlight.packed.js typescript 1 Lines Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.pulsate.packed.js typescript 1 Lines Dec 13, 2019 12:57:03

PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.scale.packed.js typescript 1 Lines 2.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.shake.packed.js typescript 1 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.slide.packed.js typescript 1 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/effects.transfer.packed.js typescript 1 Lines 1.1 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/jquery.ui.all.packed.js typescript 1 Lines 89.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.accordion.packed.js typescript 1 Lines 3.3 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.core.packed.js typescript 1 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.datepicker.packed.js typescript 1 Lines 20.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.dialog.packed.js typescript 1 Lines 4.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.draggable.packed.js typescript 1 Lines 8.7 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.droppable.packed.js typescript 1 Lines 3.6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.resizable.packed.js typescript 1 Lines 11.4 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.selectable.packed.js typescript 1 Lines 2.9 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.slider.packed.js typescript 1 Lines 6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.sortable.packed.js typescript 1 Lines 9.8 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/jquery/jquery.ui-1.5/ui/packed/ui.tabs.packed.js typescript 1 Lines 6 KB Dec 13, 2019 12:57:03 PM
omod/src/main/webapp/resources/reportingcompatibility.tld tld 1 Lines 1.2 KB Dec 13, 2019 12:57:03 PM
omod/src/test/java/org/openmrs/module/reportingcompatibility/service/ReportingCompatibilityServiceTest.java java 39 Lines 4.2 KB Dec 13, 2019 12:57:03 PM
omod/src/test/java/org/openmrs/module/reportingcompatibility/web/controller/analysis/CohortBuilderControllerTest.java java 6 Lines 1.5 KB Dec 13, 2019 12:57:03 PM
omod/src/test/java/org/openmrs/module/reportingcompatibility/web/controller/report/ReportSchemaXmlFormControllerTest.java java 33 Lines 6.3 KB Dec 13, 2019 12:57:03 PM
omod/src/test/resources/org/openmrs/include/ReportSchemaXml-otherTestData.xml xml Dec 13, 2019 12:57:03 PM
omod/src/test/resources/org/openmrs/include/drugs.xml xml 1.3 KB Dec 13, 2019 12:57:03 PM
omod/target/classes/config.xml xml 4.1 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/messages.properties java_properties 22.8 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/messages_en_GB.properties java_properties Dec 18, 2019 11:55:47 AM
omod/target/classes/messages_es.properties java_properties 13.4 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/messages_fr.properties java_properties 1.8 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/messages_it.properties java_properties 12.9 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/messages_pt.properties java_properties 1.9 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/moduleApplicationContext.xml xml 17.5 KB Dec 18, 2019 11:55:47 AM
omod/target/classes/sqldiff.xml xml Dec 18, 2019 11:55:47 AM

omod/target/classes/web/module/analysis/cohortBuilder.jsp jsp 110 Lines 63.5 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/portlets/patientSet.jsp jsp 30 Lines 8.4 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/reports/cohortList.jsp jsp 15 Lines 1.8 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/cohortReportForm.jsp jsp 44 Lines 14.4 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/dataExportForm.jsp jsp 48 Lines 28.4 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/dataExportList.jsp jsp 14 Lines 3.4 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/include/calculatedColumns.jsp jsp 1 Lines 1.2 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/include/cohortColumns.jsp jsp 6 Lines 1.8 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/include/conceptColumns.jsp jsp 1 Lines 2.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/include/simpleColumns.jsp jsp 26 Lines 9.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/localHeader.jsp jsp 19 Lines 3.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/patientSearchForm.jsp jsp 17 Lines 4.8 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/patientSearchList.jsp jsp 6 Lines 1.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportDataForm.jsp jsp 27 Lines 4.2 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportDataList.jsp jsp 11 Lines 1.3 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportMacrosForm.jsp jsp 3 Lines 1.1 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportObjectForm.jsp jsp 34 Lines 5.5 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportObjectList.jsp jsp 11 Lines 1.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportSchemaXmlForm.jsp jsp 6 Lines 1.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/reportSchemaXmlList.jsp jsp 6 Lines 1.7 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/rowPerObsDataExportForm.jsp jsp 46 Lines 28.5 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/rowPerObsDataExportList.jsp jsp 9 Lines 2.3 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/runReportForm.jsp jsp 23 Lines 2.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/reports/runReportList.jsp jsp 5 Lines 1.5 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-am.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ar.js typescript 27 Lines 2.2 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-bg.js typescript 17 Lines 1.7 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ca.js typescript 17 Lines 1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-cs.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-da.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-de.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-es.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fi.js typescript 18 Lines 1.2 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fr.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-he.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-hu.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-id.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-is.js typescript 17 Lines 1.3 KB Dec 18, 2019

11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-it.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ja.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ko.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lt.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lv.js typescript 18 Lines 1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-nl.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-no.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pl.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pt-BR.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ro.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ru.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sk.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sv.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-th.js typescript 17 Lines 1.4 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-tr.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ua.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-CN.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-TW.js typescript 18 Lines 1.3 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.blind.packed.js typescript 1 Lines Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.bounce.packed.js typescript 1 Lines 1.5 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.clip.packed.js typescript 1 Lines 1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.core.packed.js typescript 1 Lines 8.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.drop.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.explode.packed.js typescript 1 Lines 1.4 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.fold.packed.js typescript 1 Lines Dec 18, 2019 11:55:49 AM

omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.highlight.packed.js typescript 1 Lines Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.pulsate.packed.js typescript 1 Lines Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.scale.packed.js typescript 1 Lines 2.8 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.shake.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.slide.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.transfer.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/jquery.ui.all.packed.js typescript 1 Lines 89.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.accordion.packed.js typescript 1 Lines 3.3 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.core.packed.js typescript 1 Lines 3.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.datepicker.packed.js typescript 1 Lines 20.6 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.dialog.packed.js typescript 1 Lines 4.9 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.draggable.packed.js typescript 1 Lines 8.7 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.droppable.packed.js typescript 1 Lines 3.6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.resizable.packed.js typescript 1 Lines 11.4 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.selectable.packed.js typescript 1 Lines 2.9 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.slider.packed.js typescript 1 Lines 6 KB Dec 18, 2019 11:55:49 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.sortable.packed.js typescript 1 Lines 9.8 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.tabs.packed.js typescript 1 Lines 6 KB Dec 18, 2019 11:55:48 AM
omod/target/classes/web/module/resources/reportingcompatibility.tld tld 1 Lines 1.2 KB Dec 18, 2019 11:55:49 AM
omod/target/maven-archiver/pom.properties java_properties Dec 18, 2019 11:55:58 AM
omod/target/reportingcompatibility-2.0.6/config.xml xml 4.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages.properties java_properties 22.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages_en_GB.properties java_properties Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages_es.properties java_properties 13.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages_fr.properties java_properties 1.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages_it.properties java_properties 12.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/messages_pt.properties java_properties 1.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/moduleApplicationContext.xml xml 17.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/sqldiff.xml xml Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/analysis/cohortBuilder.jsp jsp 110 Lines 63.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/portlets/patientSet.jsp jsp 30 Lines 8.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortList.jsp jsp 15 Lines 1.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortReportForm.jsp jsp 44 Lines 14.4 KB Dec 18, 2019 11:56:01

AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportForm.jsp jsp 48 Lines 28.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportList.jsp jsp 14 Lines 3.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/include/calculatedColumns.jsp jsp 1 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/include/cohortColumns.jsp jsp 6 Lines 1.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/include/conceptColumns.jsp jsp 1 Lines 2.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/include/simpleColumns.jsp jsp 26 Lines 9.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/localHeader.jsp jsp 19 Lines 3.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/patientSearchForm.jsp jsp 17 Lines 4.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/patientSearchList.jsp jsp 6 Lines 1.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportDataForm.jsp jsp 27 Lines 4.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportDataList.jsp jsp 11 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportMacrosForm.jsp jsp 3 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectForm.jsp jsp 34 Lines 5.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectList.jsp jsp 11 Lines 1.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlForm.jsp jsp 6 Lines 1.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlList.jsp jsp 6 Lines 1.7 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportForm.jsp jsp 46 Lines 28.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportList.jsp jsp 9 Lines 2.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportForm.jsp jsp 23 Lines 2.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp jsp 5 Lines 1.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-am.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ar.js typescript 27 Lines 2.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-bg.js typescript 17 Lines 1.7 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ca.js typescript 17 Lines 1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-cs.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-da.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-de.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-es.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fi.js typescript 18 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-fr.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-he.js typescript 17 Lines

1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-hu.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-id.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-is.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-it.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ja.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ko.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lt.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-lv.js typescript 18 Lines 1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-nl.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-no.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pl.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-pt-BR.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ro.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ru.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sk.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-sv.js typescript 17 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-th.js typescript 17 Lines 1.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-tr.js typescript 17 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-ua.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-CN.js typescript 17 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/i18n/ui.datepicker-zh-TW.js typescript 18 Lines 1.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.blind.packed.js typescript 1 Lines Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.bounce.packed.js typescript 1 Lines 1.5 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.clip.packed.js typescript 1 Lines 1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.core.packed.js typescript 1 Lines 8.6 KB Dec 18, 2019 11:56:01 AM

omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.drop.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.explode.packed.js typescript 1 Lines 1.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.fold.packed.js typescript 1 Lines Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.highlight.packed.js typescript 1 Lines Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.pulsate.packed.js typescript 1 Lines Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.scale.packed.js typescript 1 Lines 2.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.shake.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.slide.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/effects.transfer.packed.js typescript 1 Lines 1.1 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/jquery.ui.all.packed.js typescript 1 Lines 89.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.accordion.packed.js typescript 1 Lines 3.3 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.core.packed.js typescript 1 Lines 3.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.datepicker.packed.js typescript 1 Lines 20.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.dialog.packed.js typescript 1 Lines 4.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.draggable.packed.js typescript 1 Lines 8.7 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.droppable.packed.js typescript 1 Lines 3.6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.resizable.packed.js typescript 1 Lines 11.4 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.selectable.packed.js typescript 1 Lines 2.9 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.slider.packed.js typescript 1 Lines 6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.sortable.packed.js typescript 1 Lines 9.8 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/jquery/jquery.ui-1.5/ui/packed/ui.tabs.packed.js typescript 1 Lines 6 KB Dec 18, 2019 11:56:01 AM
omod/target/reportingcompatibility-2.0.6/web/module/resources/reportingcompatibility.tld tld 1 Lines 1.2 KB Dec 18, 2019 11:56:01 AM
pom.xml xml 4.6 KB Dec 13, 2019 12:57:03 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Core, Java
Version: 2019.4.0.0009
ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF
SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, Annotations
Version: 2019.4.0.0009
ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B
SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, JavaScript
Version: 2019.4.0.0009
ID: BD292C4E-4216-4DB8-96C7-9B607BFD9584
SKU: RUL13059

Name: Fortify Secure Coding Rules, Core, Android
Version: 2019.4.0.0009
ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952
SKU: RUL13093

Name: Fortify Secure Coding Rules, Extended, JavaScript
Version: 2019.4.0.0009
ID: C4D1969E-B734-47D3-87D4-73962C1D32E2
SKU: RUL13141

Name: Fortify Secure Coding Rules, Extended, Configuration
Version: 2019.4.0.0009
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Java
Version: 2019.4.0.0009
ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317
SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2019.4.0.0009
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

Name: Fortify Secure Coding Rules, Core, Golang
Version: 2019.4.0.0009

ID: 1DCE79F8-AF6B-474D-A05A-5BFFC8B13DCD
SKU: RUL13218

Name: Fortify Secure Coding Rules, Extended, JSP
Version: 2019.4.0.0009
ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2
SKU: RUL13026

External Metadata:
Version: 2019.4.0.0009

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hiearchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like langauges and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the

National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA
The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE

The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007
ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248
The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0
ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently

allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA

STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4
ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5
ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden

or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8
ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.X11.XToolkit
com.fortify.AuthenticationKey=/home/pgupta25/.fortify/config/tools
com.fortify.Core=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core
com.fortify.InstallRoot=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0
com.fortify.InstallationUserName=pgupta25
com.fortify.SCAExecutablePath=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/bin/sourceanalyzer
com.fortify.TotalPhysicalMemory=8363917312
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=/home/pgupta25/.fortify
com.fortify.locale=en
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=reportingcompatibility
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer
com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settings,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshtml,vbhtml,inc,asp,vbscript,js,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,conf,json,yaml,yml
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/rules
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PH

PLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFileDir=/home/pgupta25/.fortify/sca19.1/log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=/home/pgupta25/.fortify/sca19.1/log/sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshtml,vbhtml
com.fortify.sca.PID=26651
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=/srv/openmrs_code/org/openmrs/module/reportingcompatibility/reportingcompatibility_scan.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=PLSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs
com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fi
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler

com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.cpfe.441.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP

com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP
com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4

com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
file.encoding=UTF-8
file.encoding.pkg=sun.io
file.separator=/
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.print.PSPrinterJob
java.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/endorsed
java.ext.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/ext:/usr/java/packages/lib/ext
java.home=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre
java.io.tmpdir=/tmp
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/log4j2.xml
log4j.isThreadContextMapInheritable=true

max.file.path.length=255
os.arch=amd64
os.name=Linux
os.version=4.15.0-58-generic
path.separator=:
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/resources.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/rt.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/sunrsasign.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jsse.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jce.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/charsets.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jfr.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/classes
sun.boot.library.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/amd64
sun.cpu.endian=little
sun.cpu.isalist=
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:SoftRefLRUPolicyMSPerMB=3000 -Dcom.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin -Dcom.fortify.sca.ProjectRoot=/home/pgupta25/.fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=26651 -Xmx4096M -Dcom.fortify.TotalPhysicalMemory=8363917312 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M -Djava.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar -scan @/home/pgupta25/.fortify/Eclipse.Plugin-19.1.0/reportingcompatibility/reportingcompatibilityScan.txt
sun.jnu.encoding=UTF-8
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=unknown
user.country=US
user.dir=/home/pgupta25/Desktop
user.home=/home/pgupta25
user.language=en
user.name=pgupta25
user.timezone=America/New_York

Commandline Arguments

-scan
-b
reportingcompatibility
-format
fpr
-machine-output
-f
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/reportingcompatibility_scan.fpr

Warnings

[12002] Could not locate the deployment descriptor (web.xml) for your web application. Please build your web application and try again. File:
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortList.jsp
[12003] Assuming Java source level to be 1.8 as it was not specified. Note that the default value may change in future versions.
[12004] The Java frontend was unable to resolve the following include:
/WEB-INF/template/include.jsp at

/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp:1.
/WEB-INF/template/footer.jsp at /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp:44.
/WEB-INF/template/header.jsp at /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp:2.
[12022] The class "javax.servlet.http.HttpServlet" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet-api-3.0.1.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.http.HttpServlet" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[12022] The class "javax.servlet.jsp.PageContext" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet.jsp-api.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.jsp.PageContext" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[1214] Multiple definitions found for class /cohortBuilder.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/analysis/cohortBuilder.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/analysis/cohortBuilder.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortBuilder_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/analysis/cohortBuilder.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/analysis/cohortBuilder.jsp).
[1214] Multiple definitions found for class /patientSet.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/portlets/patientSet.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/portlets/patientSet.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSet_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/portlets/patientSet.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/portlets/patientSet.jsp).
[1214] Multiple definitions found for class /cohortList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/cohortList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/cohortList.jsp).
[1214] Multiple definitions found for class /cohortReportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/cohortReportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortReportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/cohortReportForm.jsp).
[1214] Multiple definitions found for class /dataExportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/dataExportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspdataExportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/dataExportForm.jsp).
[1214] Multiple definitions found for class /dataExportList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/dataExportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspdataExportList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportList.jsp and

/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/dataExportList.jsp).
[1214] Multiple definitions found for class /calculatedColumns.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/calculatedColumns.jsp
and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/calculatedColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculatedColumns_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/calculatedColumns.jsp
and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/calculatedColumns.jsp).
[1214] Multiple definitions found for class /cohortColumns.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/cohortColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/cohortColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortColumns_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/cohortColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/cohortColumns.jsp).
[1214] Multiple definitions found for class /conceptColumns.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/conceptColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/conceptColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspconceptColumns_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/conceptColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/conceptColumns.jsp).
[1214] Multiple definitions found for class /simpleColumns.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/simpleColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/simpleColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspsimpleColumns_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/simpleColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/include/simpleColumns.jsp).
[1214] Multiple definitions found for class /patientSearchForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/patientSearchForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSearchForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/patientSearchForm.jsp).
[1214] Multiple definitions found for class /patientSearchList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/patientSearchList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSearchList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/patientSearchList.jsp).
[1214] Multiple definitions found for class /reportDataForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportDataForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportDataForm_jsp$ftfy_frameworkVisibleObjects

(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportDataForm.jsp).
[1214] Multiple definitions found for class /reportDataList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportDataList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportDataList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportDataList.jsp).
[1214] Multiple definitions found for class /reportMacrosForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportMacrosForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportMacrosForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportMacrosForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportMacrosForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportMacrosForm.jsp).
[1214] Multiple definitions found for class /reportObjectForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportObjectForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportObjectForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportObjectForm.jsp).
[1214] Multiple definitions found for class /reportObjectList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportObjectList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportObjectList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportObjectList.jsp).
[1214] Multiple definitions found for class /reportSchemaXmlForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportSchemaXmlForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportSchemaXmlForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportSchemaXmlForm.jsp).
[1214] Multiple definitions found for class /reportSchemaXmlList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportSchemaXmlList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportSchemaXmlList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/reportSchemaXmlList.jsp).
[1214] Multiple definitions found for class /rowPerObsDataExportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/rowPerObsDataExportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprowPerObsDataExportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/rowPerObsDataExportF

orm.jsp).
[1214] Multiple definitions found for class /rowPerObsDataExportList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportList.jsp
and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/rowPerObsDataExportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprowPerObsDataExportList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportList.jsp
and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/rowPerObsDataExportList.jsp).
[1214] Multiple definitions found for class /runReportForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/runReportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprunReportForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/runReportForm.jsp).
[1214] Multiple definitions found for class /runReportList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/runReportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprunReportList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/reports/runReportList.jsp).
[1214] Multiple definitions found for class /reportingcompatibility.tld
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/resources/reportingcompatibility.tld and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/resources/reportingcompatibility.tld).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportingcompatibility_tld$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/resources/reportingcompatibility.tld and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/classes/web/module/resources/reportingcompatibility.tld).
[1214] Multiple definitions found for class /cohortBuilder.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/analysis/cohortBuilder.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/analysis/cohortBuilder.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortBuilder_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/analysis/cohortBuilder.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/analysis/cohortBuilder.jsp).
[1214] Multiple definitions found for class /patientSet.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/portlets/patientSet.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/portlets/patientSet.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSet_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/portlets/patientSet.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/portlets/patientSet.jsp).
[1214] Multiple definitions found for class /cohortList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortList.jsp).

[1214] Multiple definitions found for class JSPPAGE._/_jspcohortList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortList.jsp).
[1214] Multiple definitions found for class /cohortReportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortReportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortReportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/cohortReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/cohortReportForm.jsp).
[1214] Multiple definitions found for class /dataExportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspdataExportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportForm.jsp).
[1214] Multiple definitions found for class /dataExportList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspdataExportList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/dataExportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/dataExportList.jsp).
[1214] Multiple definitions found for class /calculatedColumns.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/calculatedColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/include/calculatedColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcalculatedColumns_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/calculatedColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/include/calculatedColumns.jsp).
[1214] Multiple definitions found for class /cohortColumns.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/cohortColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/include/cohortColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspcohortColumns_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/cohortColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/include/cohortColumns.jsp).
[1214] Multiple definitions found for class /conceptColumns.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/conceptColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/include/conceptColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspconceptColumns_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/conceptColumns.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-

2.0.6/web/module/reports/include/conceptColumns.jsp).
[1214] Multiple definitions found for class /simpleColumns.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/simpleColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/include/simpleColumns.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspsimpleColumns_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/include/simpleColumns.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/include/simpleColumns.jsp).
[1214] Multiple definitions found for class /patientSearchForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/patientSearchForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSearchForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/patientSearchForm.jsp).
[1214] Multiple definitions found for class /patientSearchList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/patientSearchList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsppatientSearchList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/patientSearchList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/patientSearchList.jsp).
[1214] Multiple definitions found for class /reportDataForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportDataForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportDataForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportDataForm.jsp).
[1214] Multiple definitions found for class /reportDataList.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportDataList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportDataList_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportDataList.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportDataList.jsp).
[1214] Multiple definitions found for class /reportMacrosForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportMacrosForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportMacrosForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportMacrosForm_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportMacrosForm.jsp and
/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-
2.0.6/web/module/reports/reportMacrosForm.jsp).
[1214] Multiple definitions found for class /reportObjectForm.jsp
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectForm.jsp and

/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportObjectForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectForm.jsp).
[1214] Multiple definitions found for class /reportObjectList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportObjectList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportObjectList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportObjectList.jsp).
[1214] Multiple definitions found for class /reportSchemaXmlForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportSchemaXmlForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlForm.jsp).
[1214] Multiple definitions found for class /reportSchemaXmlList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportSchemaXmlList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/reportSchemaXmlList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/reportSchemaXmlList.jsp).
[1214] Multiple definitions found for class /rowPerObsDataExportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprowPerObsDataExportForm_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportForm.jsp).
[1214] Multiple definitions found for class /rowPerObsDataExportList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprowPerObsDataExportList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/rowPerObsDataExportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/rowPerObsDataExportList.jsp).
[1214] Multiple definitions found for class /runReportForm.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportForm.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprunReportForm_jsp$ftfy_frameworkVisibleObjects

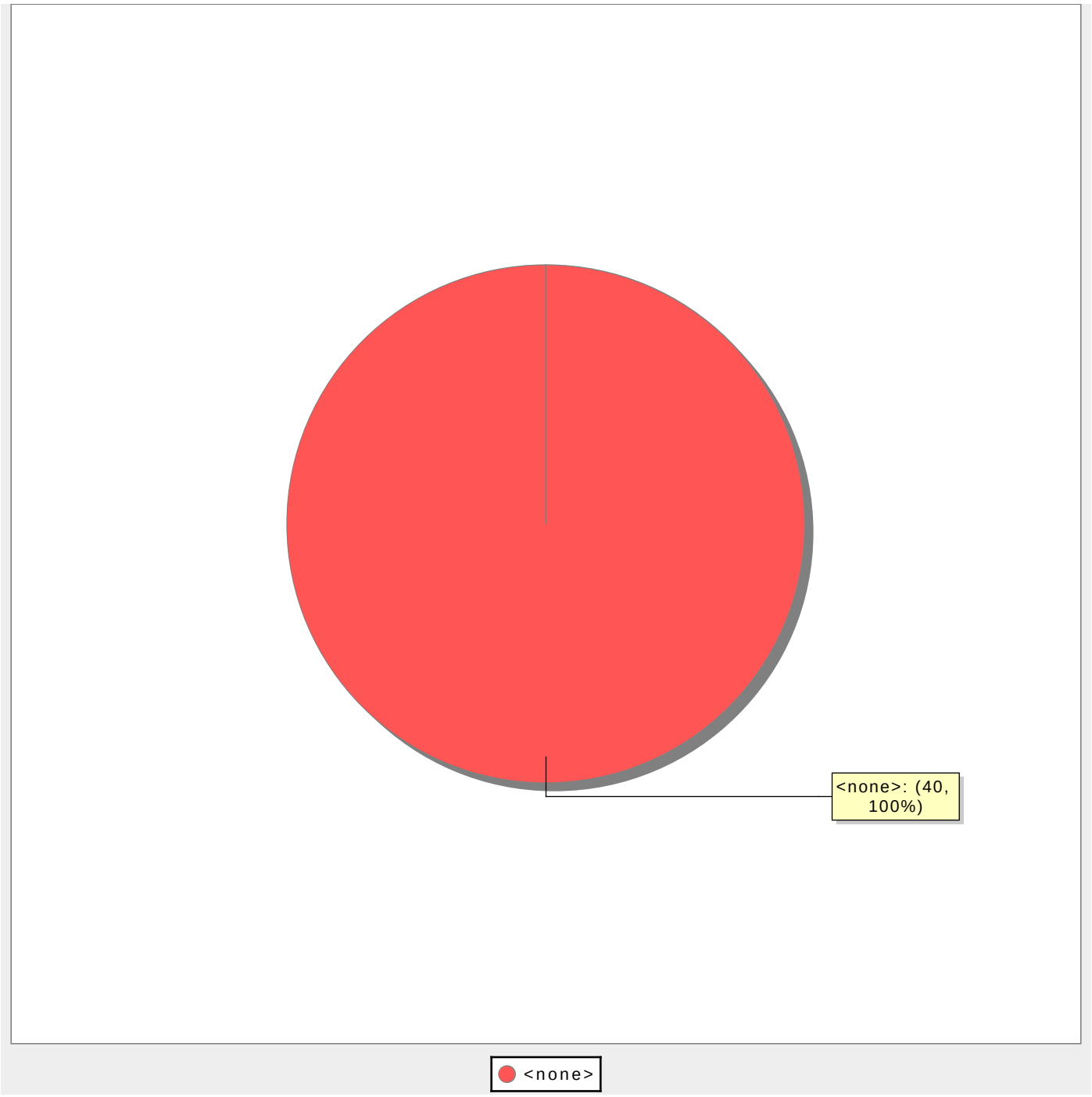
(/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportForm.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportForm.jsp).
[1214] Multiple definitions found for class /runReportList.jsp (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jsprunReportList_jsp$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/reports/runReportList.jsp and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/reports/runReportList.jsp).
[1214] Multiple definitions found for class /reportingcompatibility.tld (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/resources/reportingcompatibility.tld and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/resources/reportingcompatibility.tld).
[1214] Multiple definitions found for class JSPPAGE._/_jspreportingcompatibility_tld$ftfy_frameworkVisibleObjects (/srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/src/main/webapp/resources/reportingcompatibility.tld and /srv/openmrs_code/org/openmrs/module/reportingcompatibility/omod/target/reportingcompatibility-2.0.6/web/module/resources/reportingcompatibility.tld).
[1215] Could not locate the root (WEB-INF) of the web application. Please build your web application and try again.

Issue Count by Category

Issues by Category	
Log Forging	21
Cross-Site Scripting: Reflected	15
Denial of Service: Regular Expression	2
Dynamic Code Evaluation: XMLDecoder Injection	1
XML External Entity Injection	1

Issue Breakdown by Analysis

Issues by Analysis



Fortify Security Report

Jan 29, 2020

skumar32

Executive Summary

Issues Overview

On Jan 29, 2020, a source code review was performed over the uiframework code base. 260 files, 3,065 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 5 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
High	3
Critical	2

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: /srv/openmrs_code/org/openmrs/module/uiframework
Number of Files: 260
Lines of Code: 3065
Build Label: <No Build Label>

Scan Information

Scan time: 04:23
SCA Engine version: 19.1.0.2241
Machine Name: vclv98-235.hpc.ncsu.edu
Username running scan: skumar32

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
File System:
java.io.FileInputStream.FileInputStream
java.io.FileInputStream.FileInputStream

System Information:
null.null.null
java.lang.ClassLoader.getResource
java.lang.System.getProperty
java.lang.Throwable.getMessage
org.openmrs.ui.framework.AttributeExpressionException.getMessage
org.openmrs.ui.framework.MissingRequiredParameterException.getMessage

Web:
javax.servlet.http.HttpServletRequest.getMethod

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
If impact is not in range [2.5, 5.0] Then hide issue
If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

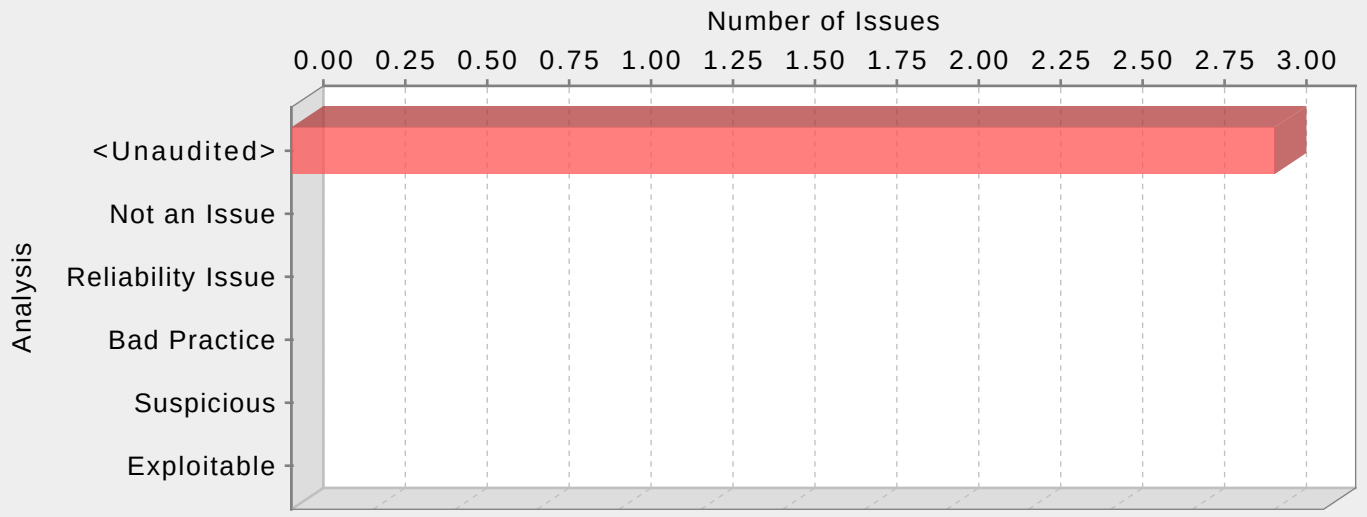
Results Outline

Overall number of results

The scan found 5 issues.

Vulnerability Examples by Category

Category: Log Forging (3 Issues)



Abstract:

The method render() in GroovyFragmentView.java writes unvalidated user input to the log on line 42. An attacker could take advantage of this behavior to forge log entries or inject malicious content into the log.

Explanation:

Log forging vulnerabilities occur when:

1. Data enters an application from an untrusted source.

2. The data is written to an application or system log file.

Applications typically use log files to store a history of events or transactions for later review, statistics gathering, or debugging. Depending on the nature of the application, the task of reviewing log files may be performed manually on an as-needed basis or automated with a tool that automatically culls logs for important events or trending information.

Interpretation of the log files may be hindered or misdirected if an attacker can supply data to the application that is subsequently logged verbatim. In the most benign case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker may be able to render the file unusable by corrupting the format of the file or injecting unexpected characters. A more subtle attack might involve skewing the log file statistics. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to implicate another party in the commission of a malicious act [1]. In the worst case, an attacker may inject code or other commands into the log file and take advantage of a vulnerability in the log processing utility [2].

Example 1: The following web application code attempts to read an integer value from a request object. If the value fails to parse as an integer, then the input is logged with an error message indicating what happened.

```
...
String val = request.getParameter("val");
try {
int value = Integer.parseInt(val);
}
catch (NumberFormatException nfe) {
log.info("Failed to parse val = " + val);
}
...
```

If a user submits the string "twenty-one" for val, the following entry is logged:

INFO: Failed to parse val=twenty-one

However, if an attacker submits the string "twenty-one%0a%0aINFO:+User+logged+out%3dbadguy", the following entry is logged:

INFO: Failed to parse val=twenty-one

INFO: User logged out=badguy

Clearly, attackers may use this same mechanism to insert arbitrary log entries.

Some think that in the mobile world, classic web application vulnerabilities, such as log forging, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 2: The following code adapts Example 1 to the Android platform.

```
...
String val = this.getIntent().getExtras().getString("val");
try {
int value = Integer.parseInt();
}
catch (NumberFormatException nfe) {
Log.e(TAG, "Failed to parse val = " + val);
}
...
```

Recommendations:

Prevent log forging attacks with indirection: create a set of legitimate log entries that correspond to different events that must be logged and only log entries from this set. To capture dynamic content, such as users logging out of the system, always use server-controlled values rather than user-supplied data. This ensures that the input provided by the user is never used directly in a log entry.

Example 1 can be rewritten to use a pre-defined log entry that corresponds to a NumberFormatException as follows:

```
...
public static final String NFE = "Failed to parse val. The input is required to be an integer value."
...
String val = request.getParameter("val");
try {
int value = Integer.parseInt(val);
}
catch (NumberFormatException nfe) {
log.info(NFE);
}
..
```

And here is an Android equivalent:

```
...
public static final String NFE = "Failed to parse val. The input is required to be an integer value."
...
String val = this.getIntent().getExtras().getString("val");
try {
int value = Integer.parseInt();
}
catch (NumberFormatException nfe) {
Log.e(TAG, NFE);
}
...
```

In some situations this approach is impractical because the set of legitimate log entries is too large or complicated. In these situations, developers often fall back on blacklisting. Blacklisting selectively rejects or escapes potentially dangerous characters before using the input. However, a list of unsafe characters can quickly become incomplete or outdated. A better approach is to create a whitelist of characters that are allowed to appear in log entries and accept input composed exclusively of characters in the approved set. The most critical character in most log forging attacks is the '\n' (newline) character, which should never appear on a log entry whitelist.

Tips:

1. Many logging operations are created only for the purpose of debugging a program during development and testing. In our experience, debugging will be enabled, either accidentally or purposefully, in production at some point. Do not excuse log forging vulnerabilities simply because a programmer says "I don't have any plans to turn that on in production".

2. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, the Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

GroovyFragmentView.java, line 42 (Log Forging)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method render() in GroovyFragmentView.java writes unvalidated user input to the log on line 42. An attacker could take advantage of this behavior to forge log entries or inject malicious content into the log.		

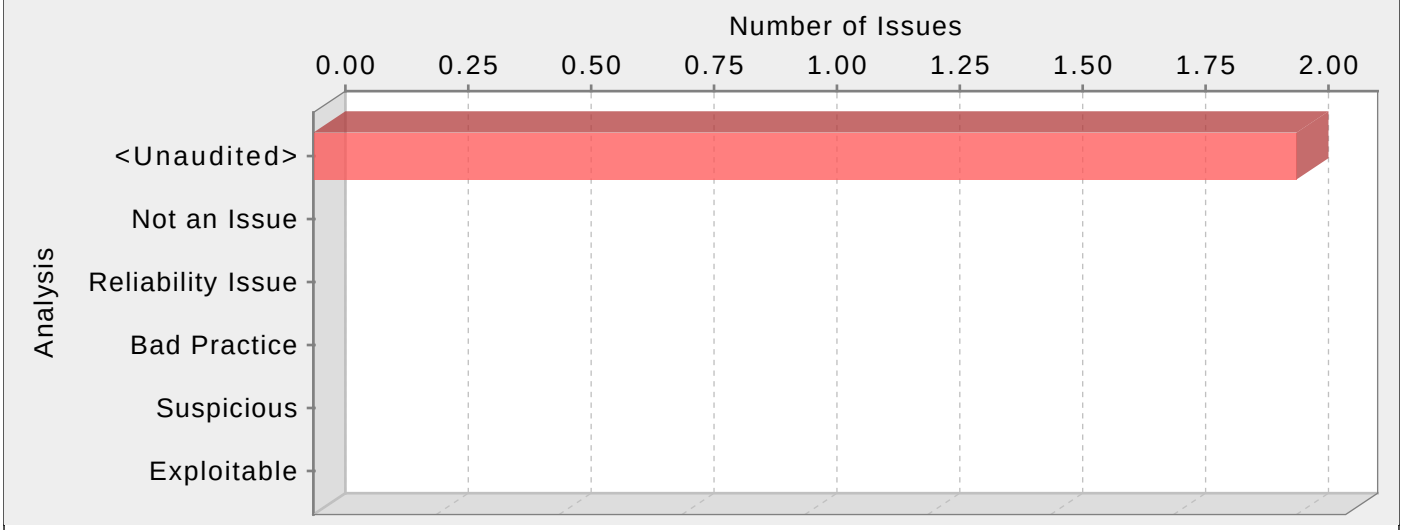
Source: PageController.java:174 javax.servlet.http.HttpServletRequest.getQueryString()

```
172     private void setRedirectUrl(HttpServletRequest request) {
173       StringBuffer url = request.getRequestURL();
174       String queryStr = request.getQueryString();
175       if (StringUtils.isNotBlank(queryStr)) {
176         url = url.append("?").append(queryStr);
```

Sink: GroovyFragmentView.java:42 org.apache.commons.logging.Log.trace()

```
40    Writable boundTemplate = model == null ? template.make() : template.make(model);
41    if (log.isTraceEnabled())
42      log.trace("rendering groovy fragment view with model: " + model);
43    // TODO add a way for the view to redirect. Perhaps this should happen via the context
44    // instead of via a return value
```

Category: Path Manipulation (2 Issues)



Abstract:

Attackers are able to control the file system path argument to File() at ModuleResourceProvider.java line 45, which allows them to access or modify otherwise protected files.

Explanation:

Path manipulation errors occur when the following two conditions are met:

1. An attacker is able to specify a path used in an operation on the file system.

2. By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

For example, the program may give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.

Example 1: The following code uses input from an HTTP request to create a file name. The programmer has not considered the possibility that an attacker could provide a file name such as "../../tomcat/conf/server.xml", which causes the application to delete one of its own configuration files.

```
String rName = request.getParameter("reportName");
File rFile = new File("/usr/local/apfr/reports/" + rName);
...
rFile.delete();
```

Example 2: The following code uses input from a configuration file to determine which file to open and echo back to the user. If the program runs with adequate privileges and malicious users can change the configuration file, they can use the program to read any file on the system that ends with the extension .txt.

```
fis = new FileInputStream(cfg.getProperty("sub")+".txt");
amt = fis.read(arr);
out.println(arr);
```

Some think that in the mobile world, classic vulnerabilities, such as path manipulation, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 3: The following code adapts Example 1 to the Android platform.

```
...
String rName = this.getIntent().getExtras().getString("reportName");
File rFile = getBaseContext().getFileStreamPath(rName);
...
rFile.delete();
...
```

Recommendations:

The best way to prevent path manipulation is with a level of indirection: create a list of legitimate resource names that a user is allowed to specify, and only allow the user to select from the list. With this approach the input provided by the user is never used directly to specify the resource name.

In some situations this approach is impractical because the set of legitimate resource names is too large or too hard to keep track of. Programmers often resort to blacklisting in these situations. Blacklisting selectively rejects or escapes potentially dangerous characters before using the input. However, any such list of unsafe characters is likely to be incomplete and will almost certainly become out of date. A better approach is to create a whitelist of characters that are allowed to appear in the resource name and accept input composed exclusively of characters in the approved set.

Tips:

1. If the program is performing custom input validation you are satisfied with, use the Fortify Custom Rules Editor to create a cleanse rule for the validation routine.

2. Implementation of an effective blacklist is notoriously difficult. One should be skeptical if validation logic requires blacklisting. Consider different types of input encoding and different sets of meta-characters that might have special meaning when interpreted by different operating systems, databases, or other resources. Determine whether or not the blacklist can be updated easily, correctly, and completely if these requirements ever change.

3. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, the Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

ModuleResourceProvider.java, line 45 (Path Manipulation)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	Attackers are able to control the file system path argument to File() at ModuleResourceProvider.java line 45, which allows them to access or modify otherwise protected files.		

Source: ResourceServlet.java:94 javax.servlet.http.HttpServletRequest.getPathInfo()

```
92    ResourceFactory factory = ResourceFactory.getInstance();
93
94    String path = request.getPathInfo();
95    try {
96     // path is like "/uiframework/resource/providerName/path/to/resource.png"
```

Sink: ModuleResourceProvider.java:45 java.io.File.File()

```
43     for (File developmentFolder : developmentFolders) {
44         // we're in development mode, and we want to dynamically reload resource from this
filesystem directory
45      File file = new File(developmentFolder, path);
46      if (file.exists()) {
47       return file;
```

Detailed Project Summary

Files Scanned

Code base location: /srv/openmrs_code/org/openmrs/module/uiframework

Files Scanned:

.travis.yml yaml Dec 13, 2019 12:56:24 PM

api/pom.xml xml 2.6 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/module/uiframework/UiFrameworkActivator.java java 22 Lines 3.5 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/module/uiframework/UiFrameworkConversionServiceFactoryBean.java java 2 Lines 1.4 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/AttributeExpressionException.java java 10 Lines 1.2 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/AttributeHolder.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/AttributeHolderUtil.java java 12 Lines 2.1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/BasicUiUtils.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/BindParamsValidationException.java java 17 Lines 1.3 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/CodedOrFreeTextValue.java java 32 Lines 3.2 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/Decoratable.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/DevelopmentClassLoader.java java 15 Lines 1.9 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/Formatter.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/FormatterImpl.java java 109 Lines 12.4 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/FragmentException.java java 3 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/FragmentIncluder.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/Link.java java 11 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/Messager.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/MessagerImpl.java java 4 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/MissingRequiredCookieException.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/MissingRequiredParameterException.java java 5 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/MockMessageSource.java java 9 Lines 1.9 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/Model.java java 9 Lines 1.5 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/NameSupportCompatibility.java java 18 Lines 1.6 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/ProviderAndName.java java 7 Lines 1.3 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/RequestValidationException.java java 7 Lines 1.1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/ResourceIncluder.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/SimpleObject.java java 59 Lines 7.3 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/StandardModuleUiConfiguration.java java 35 Lines 4.9 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UiContextRefreshedCallback.java java 1.3 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UiFrameworkConstants.java java 5 Lines 1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UiFrameworkException.java java 4 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UiFrameworkUtil.java java 222 Lines 29.2 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UiUtils.java java 152 Lines 18.7 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/UserDefinedPageView.java java 19 Lines 3.2 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/ViewException.java java 3 Lines Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/WebConstants.java java 20 Lines 1.9 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/BindParams.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/FragmentParam.java java 1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/InjectBeans.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/MethodParam.java java 1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/SpringBean.java java 1.1 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/annotation/Validate.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/converter/ConceptNumericToConceptConverter.java java 2 Lines 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/MultipartFileToInputStreamConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/OpenmrsMetadataToSimpleObjectConverter.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/OpenmrsObjectToSimpleObjectConverter.java java 5 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/OpenmrsObjectToStringConverter.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/PatientIdentifierToSimpleObjectConverter.java java 8 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/PatientToSimpleObjectConverter.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToArrayNodeConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToCodedOrFreeTextValueConverter.java java 9 Lines 3.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToConceptConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToConceptNameConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToDateConverter.java java 13 Lines 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToDrugOrderConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToEncounterConverter.java java 5 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToEncounterTypeConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToFormConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToGlobalPropertyConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToJsonNodeConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToLocationAttributeTypeConverter.java java 4 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToLocationConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToLocationTagConverter.java java 4 Lines 1.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToObjectNodeConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToOrderConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPatientConverter.java java 5 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPatientIdentifierConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPatientIdentifierTypeConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPatientProblemConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPatientProgramConverter.java java 2 Lines 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPersonAttributeConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPersonAttributeTypeConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPersonConverter.java java 4 Lines 1.1 KB Dec 13, 2019 12:56:24

PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToPrivilegeConverter.java java 3 Lines 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToProgramConverter.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToProviderAttributeTypeConverter.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToProviderConverter.java java 4 Lines 1.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToRelationshipConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToRelationshipTypeConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToRoleConverter.java java 5 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToUserConverter.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToVisitConverter.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/StringToVisitTypeConverter.java java 4 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/converter/util/ConversionUtil.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/db/SingleClassDAO.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/db/UserDefinedPageViewDAO.java java 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/db/hibernate/HibernateUserDefinedPageViewDAO.java java 3 Lines 1.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/db/hibernate/SingleClassHibernateDAO.java java 8 Lines 1.8 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/EncounterHandlingFormEntryExtension.java java 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/Extension.java java 2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/ExtensionAware.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/ExtensionFactory.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/ExtensionManager.java java 39 Lines 6.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/ExtensionPoint.java java 11 Lines 1.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/ExtensionPointFactory.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/FormEntryExtension.java java 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/LinkExtension.java java 12 Lines 1.7 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/MapResourceExtension.java java 15 Lines 1.8 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/PatientExtension.java java 10 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/PatientFragmentExtension.java java 11 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/SpringBeanExtensionFactory.java java 3 Lines 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/extension/TopLevelAppExtension.java java 1 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/formatter/FormatterFactory.java java 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/formatter/FormatterService.java java 19 Lines 4.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/formatter/HandlebarsFormatterFactory.java java 6 Lines 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/formatter/TemplateFormatterFactory.java java 8 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/CompoundFragmentView.java java 17 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/ConventionBasedClasspathFragmentControllerProvider.java java 25 Lines 2.5 KB Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/fragment/EmptyFragmentController.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/Fragment.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentActionRequest.java java 28 Lines 2.9 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentActionUiUtils.java java 5 Lines 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentConfiguration.java java 15 Lines 2.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentContext.java java 28 Lines 4 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentControllerProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentFactory.java java 192 Lines 23.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentModel.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentModelConfigurator.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentRequest.java java 20 Lines 2.9 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentRequestMapper.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentUiUtils.java java 17 Lines 1.8 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentView.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/FragmentViewProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/GroovyFragmentView.java java 32 Lines 3.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/GroovyFragmentViewProvider.java java 39 Lines 4.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/PossibleFragmentActionArgumentProvider.java java 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/PossibleFragmentControllerArgumentProvider.java java 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/SpringMvcPageAsFragmentViewProvider.java java 8 Lines 2.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/action/FailureResult.java java 22 Lines 2.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/action/FragmentActionResult.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/action/ObjectResult.java java 6 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/fragment/action/SuccessResult.java java 5 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/interceptor/FragmentActionInterceptor.java java 1.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/interceptor/PageRequestInterceptor.java java 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/notification/Notification.java java 14 Lines 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/notification/NotificationManager.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/notification/NotificationManagerImpl.java java 5 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/notification/NotificationProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/ConventionBasedClasspathPageControllerProvider.java java 25 Lines 2.5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/EmptyPageController.java java 1 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/FileDownload.java java 11 Lines 1.8 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/GlobalResourceIncluder.java java 9 Lines 2.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/GroovyPageView.java java 28 Lines 2.7 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/GroovyPageViewProvider.java java 37 Lines 5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageAction.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageContext.java java 75 Lines 8.9 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageControllerProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageFactory.java java 114 Lines 15.1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageModel.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageModelConfigurator.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageRequest.java java 30 Lines 5 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageRequestMapper.java java Dec 13, 2019 12:56:24 PM

api/src/main/java/org/openmrs/ui/framework/page/PageUiUtils.java java 9 Lines 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageView.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PageViewProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/PossiblePageControllerArgumentProvider.java java 1 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/Redirect.java java 13 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/SingleCompoundFragmentPageView.java java 11 Lines 1.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/SpringMvcPageViewProvider.java java 11 Lines 2.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/SpringMvcView.java java 43 Lines 6.9 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/page/UserDefinedPageViewProvider.java java 15 Lines 2.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/resource/ModuleResourceProvider.java java 19 Lines 3.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/resource/Resource.java java 28 Lines 3.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/resource/ResourceFactory.java java 25 Lines 4.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/resource/ResourceProvider.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/session/BaseSessionListener.java java 1 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/session/Session.java java 12 Lines 1.6 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/session/SessionFactory.java java 28 Lines 3.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/session/SessionListener.java java Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/framework/util/DateExt.java java 36 Lines 2.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/util/ByFormattedObjectComparator.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/main/java/org/openmrs/ui/util/ExceptionUtil.java java 6 Lines Dec 13, 2019 12:56:24 PM
api/src/main/resources/UserDefinedPageView.hbm.xml xml 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/main/resources/liquibase.xml xml 1.3 KB Dec 13, 2019 12:56:24 PM
api/src/main/resources/messages.properties java_properties Dec 13, 2019 12:56:24 PM
api/src/main/resources/messages_de.properties java_properties Dec 13, 2019 12:56:24 PM
api/src/main/resources/messages_fr.properties java_properties Dec 13, 2019 12:56:24 PM
api/src/main/resources/messages_ht.properties java_properties Dec 13, 2019 12:56:24 PM
api/src/main/resources/moduleApplicationContext.xml xml Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/AttributeHolderUtilTest.java java 13 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/FormatterImplTest.java java 55 Lines 7.1 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/MockDomainObject.java java 7 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/MockDomainSubclass.java java 1 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/SimpleObjectTest.java java 38 Lines 4.6 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/UiFrameworkUtilTest.java java 117 Lines 13.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/UiUtilsTest.java java 34 Lines 4.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToArrayNodeConverterTest.java java 3 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToCodedOrFreeTextValueConverterTest.java java 19 Lines 3.9 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToEncounterConverterTest.java java 7 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToGlobalPropertyConverterTest.java java 9 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToJsonNodeConverterTest.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToObjectNodeConverterTest.java java 2 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToPatientConverterTest.java java 7 Lines 1.5 KB Dec 13, 2019

12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/converter/StringToProgramConverterTest.java java 4 Lines Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/db/UserDefinedPageViewDAOTest.java java 2 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/formatter/FormatterServiceTest.java java 30 Lines 3.6 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/fragment/FragmentFactoryTest.java java 98 Lines 13.3 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/fragment/FragmentRequestTest.java java 9 Lines 1.2 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/page/GroovyPageViewProviderTest.java java 5 Lines 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/page/PageContextTest.java java 31 Lines 3.1 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/page/PageFactoryTest.java java 83 Lines 10.2 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/page/SpringMvcViewTest.java java 9 Lines 2.2 KB Dec 13, 2019 12:56:24 PM
api/src/test/java/org/openmrs/ui/framework/util/DateExtTest.java java 31 Lines 2.9 KB Dec 13, 2019 12:56:24 PM
api/src/test/resources/ModuleTestData-userDefinedPageViews.xml xml Dec 13, 2019 12:56:24 PM
api/src/test/resources/TestingApplicationContext.xml xml 1.4 KB Dec 13, 2019 12:56:24 PM
api/src/test/resources/test-hibernate.cfg.xml xml Dec 13, 2019 12:56:24 PM
api/target/classes/UserDefinedPageView.hbm.xml xml 1.2 KB Dec 18, 2019 12:13:22 PM
api/target/classes/liquibase.xml xml 1.3 KB Dec 18, 2019 12:13:22 PM
api/target/classes/messages.properties java_properties Dec 18, 2019 12:13:22 PM
api/target/classes/messages_de.properties java_properties Dec 18, 2019 12:13:22 PM
api/target/classes/messages_fr.properties java_properties Dec 18, 2019 12:13:22 PM
api/target/classes/messages_ht.properties java_properties Dec 18, 2019 12:13:22 PM
api/target/classes/moduleApplicationContext.xml xml Dec 18, 2019 12:13:22 PM
api/target/maven-archiver/pom.properties java_properties Dec 18, 2019 12:13:28 PM
omod-2.0/pom.xml xml Dec 13, 2019 12:56:24 PM
omod-2.0/src/main/java/org/openmrs/module/uiframework/UrlMappingsRegistrar.java java 7 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
omod-2.0/target/maven-archiver/pom.properties java_properties Dec 18, 2019 12:13:29 PM
omod/pom.xml xml 5.8 KB Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/FragmentActionController.java java 93 Lines 14.5 KB Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/PageController.java java 55 Lines 7.7 KB Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/ResourceServlet.java java 27 Lines 3.4 KB Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/fragment/controller/HelloUserFragmentController.java java 1 Lines Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/page/controller/FragmentPageController.java java 10 Lines 1.5 KB Dec 13, 2019 12:56:24 PM
omod/src/main/java/org/openmrs/module/uiframework/page/controller/HomePageController.java java 2 Lines Dec 13, 2019 12:56:24 PM
omod/src/main/resources/config.xml xml 2.7 KB Dec 13, 2019 12:56:24 PM
omod/src/main/resources/webModuleApplicationContext.xml xml 5.3 KB Dec 13, 2019 12:56:24 PM
omod/src/main/webapp/showHtml.jsp jsp 1 Lines Dec 13, 2019 12:56:24 PM
omod/src/main/webapp/uiError.jsp jsp 3 Lines Dec 13, 2019 12:56:24 PM
omod/src/test/java/org/openmrs/ui/framework/IntegrationTest.java java 19 Lines 5 KB Dec 13, 2019 12:56:24 PM
omod/src/test/java/org/openmrs/ui/framework/PageControllerTest.java java 14 Lines 2.4 KB Dec 13, 2019 12:56:24 PM
omod/src/test/java/org/openmrs/ui/framework/test/ClassWithAutowiredAnnotations.java java 1 Lines 1.2 KB Dec 13, 2019 12:56:24 PM
omod/target/classes/META-INF/maven/org.openmrs.module/uiframework-api/pom.properties java_properties Dec 18, 2019 12:13:28 PM
omod/target/classes/META-INF/maven/org.openmrs.module/uiframework-api/pom.xml xml 2.6 KB Dec 13, 2019 12:56:24 PM
omod/target/classes/UserDefinedPageView.hbm.xml xml 1.2 KB Dec 18, 2019 12:13:22 PM
omod/target/classes/config.xml xml 2.7 KB Dec 18, 2019 12:13:31 PM

omod/target/classes/liquibase.xml xml 1.3 KB Dec 18, 2019 12:13:22 PM
omod/target/classes/messages.properties java_properties Dec 18, 2019 12:13:22 PM
omod/target/classes/messages_de.properties java_properties Dec 18, 2019 12:13:22 PM
omod/target/classes/messages_fr.properties java_properties Dec 18, 2019 12:13:22 PM
omod/target/classes/messages_ht.properties java_properties Dec 18, 2019 12:13:22 PM
omod/target/classes/moduleApplicationContext.xml xml Dec 18, 2019 12:13:22 PM
omod/target/classes/web/module/showHtml.jsp jsp 1 Lines Dec 18, 2019 12:13:31 PM
omod/target/classes/web/module/uiError.jsp jsp 3 Lines Dec 18, 2019 12:13:31 PM
omod/target/classes/webModuleApplicationContext.xml xml 5.3 KB Dec 18, 2019 12:13:31 PM
omod/target/maven-archiver/pom.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/META-INF/maven/org.openmrs.module/uiframework-api/pom.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/META-INF/maven/org.openmrs.module/uiframework-api/pom.xml xml 2.6 KB Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/UserDefinedPageView.hbm.xml xml 1.2 KB Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/config.xml xml 2.7 KB Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/liquibase.xml xml 1.3 KB Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/messages.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/messages_de.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/messages_fr.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/messages_ht.properties java_properties Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/moduleApplicationContext.xml xml Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/web/module/showHtml.jsp jsp 1 Lines Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/web/module/uiError.jsp jsp 3 Lines Dec 18, 2019 12:13:32 PM
omod/target/uiframework-3.15.0/webModuleApplicationContext.xml xml 5.3 KB Dec 18, 2019 12:13:32 PM
pom.xml xml 9.3 KB Dec 13, 2019 12:56:24 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Core, Java
Version: 2019.4.0.0009
ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF
SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, Annotations
Version: 2019.4.0.0009
ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B
SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, Android

Version: 2019.4.0.0009
ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952
SKU: RUL13093

Name: Fortify Secure Coding Rules, Extended, Configuration
Version: 2019.4.0.0009
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Java
Version: 2019.4.0.0009
ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317
SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2019.4.0.0009
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

Name: Fortify Secure Coding Rules, Core, Golang
Version: 2019.4.0.0009
ID: 1DCE79F8-AF6B-474D-A05A-5BFFC8B13DCD
SKU: RUL13218

Name: Fortify Secure Coding Rules, Extended, JSP
Version: 2019.4.0.0009
ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2
SKU: RUL13026

External Metadata:
Version: 2019.4.0.0009

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hiearchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like langauges and the software under analysis might not be within the C-family of languages -

thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the

MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA
The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE
The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007
ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248

The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0
ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden

or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4
ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5
ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority

Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8
ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>

<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.X11.XToolkit
com.fortify.AuthenticationKey=/home/skumar32/.fortify/config/tools
com.fortify.Core=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core
com.fortify.InstallRoot=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0
com.fortify.InstallationUserName=skumar32
com.fortify.SCAExecutablePath=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/bin/sourceanalyzer
com.fortify.TotalPhysicalMemory=8363909120
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=/home/skumar32/.fortify
com.fortify.locale=en
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=uiframework
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer

com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settings,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshtml,vbhtml,inc,asp,vbscript,js,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,conf,json,yaml,yml
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/rules
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PHPLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx6216425472 -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFileDir=/home/skumar32/.fortify/sca19.1/log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=/home/skumar32/.fortify/sca19.1/log/sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshtml,vbhtml
com.fortify.sca.PID=4647
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=/home/skumar32/.fortify
com.fortify.sca.ProjectRoot=/home/skumar32/.fortify
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=/srv/openmrs_code/org/openmrs/module/uiframework/uiframework_scan.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=PLSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60

com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs
com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fi
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.cpfe.441.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused

com.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP
com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP
com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP

com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4
com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
file.encoding=UTF-8
file.encoding.pkg=sun.io
file.separator=/
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.print.PSPrinterJob
java.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/endorsed
java.ext.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/ext:/usr/java/packages/lib/ext
java.home=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre
java.io.tmpdir=/tmp
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib

java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/log4j2.xml
log4j.isThreadContextMapInheritable=true
max.file.path.length=255
os.arch=amd64
os.name=Linux
os.version=4.15.0-58-generic
path.separator=:
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/resources.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/rt.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/sunrsasign.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jsse.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jce.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/charsets.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jfr.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/classes
sun.boot.library.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/amd64
sun.cpu.endian=little
sun.cpu.isalist=
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:SoftRefLRUPolicyMSPerMB=3000 -Dcom.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin -Dcom.fortify.sca.ProjectRoot=/home/skumar32/.fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=4647 -Xmx6216425472 -Dcom.fortify.TotalPhysicalMemory=8363909120 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx6216425472 -Xss16M -Djava.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar -scan @/home/skumar32/.fortify/Eclipse.Plugin-19.1.0/uiframework/uiframeworkScan.txt
sun.jnu.encoding=UTF-8
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=unknown
user.country=US
user.dir=/home/skumar32
user.home=/home/skumar32
user.language=en

user.name=skumar32
user.timezone=America/New_York

Commandline Arguments

-scan
-b
uiframework
-format
fpr
-machine-output
-f
/srv/openmrs_code/org/openmrs/module/uiframework/uiframework_scan.fpr

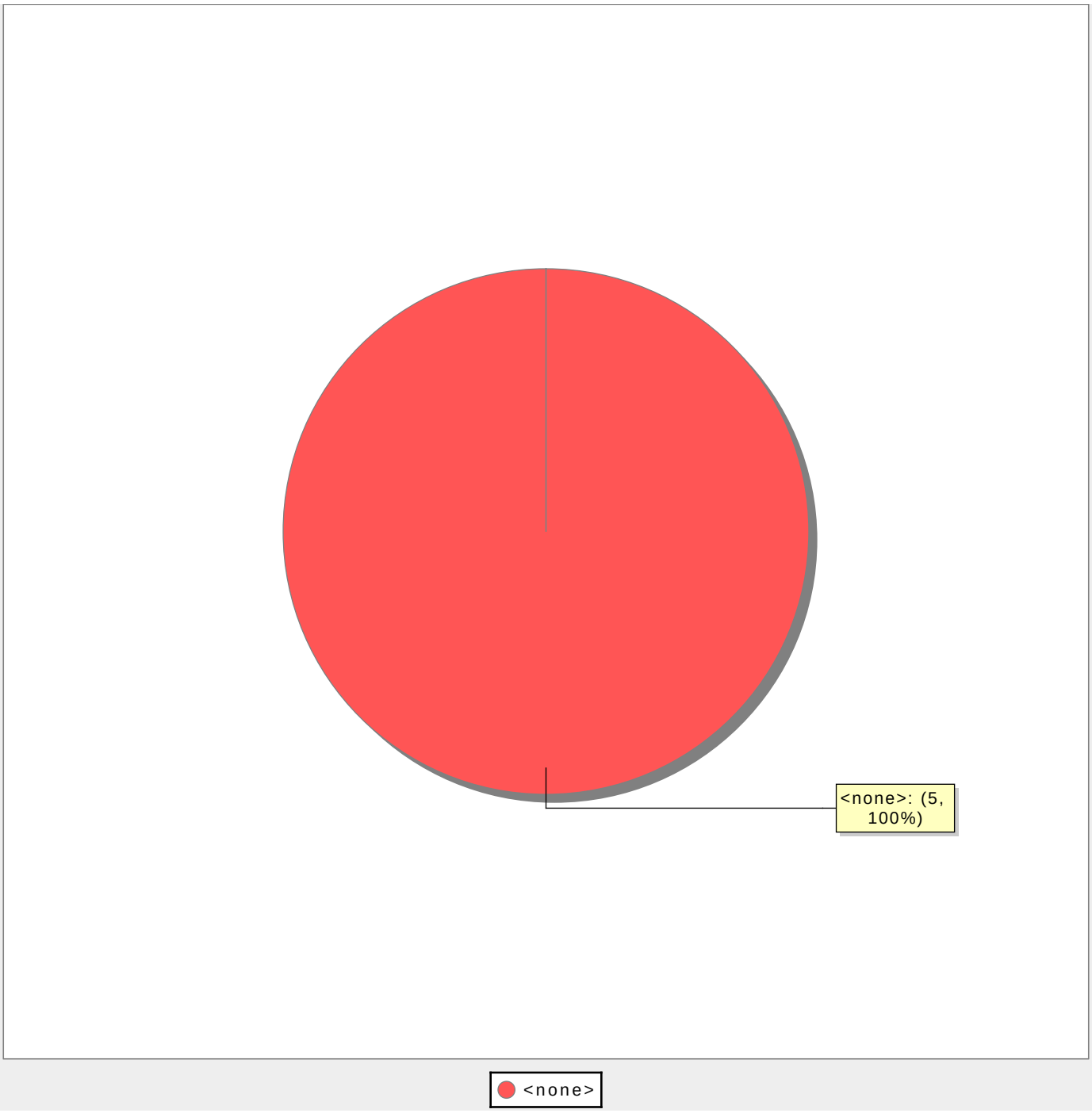
Warnings

[12003] Assuming Java source level to be 1.8 as it was not specified. Note that the default value may change in future versions.
[12022] The class "javax.servlet.http.HttpServlet" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet-api-3.0.1.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.http.HttpServlet" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[12022] The class "javax.servlet.jsp.PageContext" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/default_jars/javax.servlet.jsp-api.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.jsp.PageContext" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[1214] Multiple definitions found for class /showHtml.jsp
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/showHtml.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/classes/web/module/showHtml.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspshowHtml_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/showHtml.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/classes/web/module/showHtml.jsp).
[1214] Multiple definitions found for class /uiError.jsp
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/uiError.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/classes/web/module/uiError.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspuiError_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/uiError.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/classes/web/module/uiError.jsp).
[1214] Multiple definitions found for class /showHtml.jsp
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/showHtml.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/uiframework-3.15.0/web/module/showHtml.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspshowHtml_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/showHtml.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/uiframework-3.15.0/web/module/showHtml.jsp).
[1214] Multiple definitions found for class /uiError.jsp
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/uiError.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/uiframework-3.15.0/web/module/uiError.jsp).
[1214] Multiple definitions found for class JSPPAGE._/_jspuiError_jsp$ftfy_frameworkVisibleObjects
(/srv/openmrs_code/org/openmrs/module/uiframework/omod/src/main/webapp/uiError.jsp and
/srv/openmrs_code/org/openmrs/module/uiframework/omod/target/uiframework-3.15.0/web/module/uiError.jsp).
[1215] Could not locate the root (WEB-INF) of the web application. Please build your web application and try again.

Issue Count by Category	
Issues by Category	
Log Forging	3
Path Manipulation	2

Issue Breakdown by Analysis

Issues by Analysis



CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
10573	Filesystem path, filename, or URI manipulation	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	22
10576	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
10595	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
10682	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
10709	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
12474	Unsafe deserialization	High	01/25/20	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
12480	Unsafe deserialization	High	01/25/20	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
12482	Unsafe deserialization	High	01/25/20	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
11018	Resource leak on an exceptional path	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Exceptional resource leaks	Various	404
12486	Resource leak on an exceptional path	Low	01/26/20	Unassigned	Unclassified	Unspecified	Undecided	Other	Exceptional resource leaks	Various	404
11008	Filesystem path, filename, or URI manipulation	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	22
11060	Filesystem path, filename, or URI manipulation	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	22
11025	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11028	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11039	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
10995	Open redirect	Medium	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Medium impact security	Security	601
10996	SQL injection	Medium	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Medium impact security	Security	89
11016	Open redirect	Medium	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Medium impact security	Security	601
11031	SQL injection	Medium	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Medium impact security	Security	89
10939	Resource leak	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	Various	404
10972	Resource leak	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	Various	404
10984	Resource leak	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	Various	404
10992	Resource leak	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	Various	404
11006	Resource leak	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	Various	404

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
11096	Cross-site request forgery	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	352
11097	Cross-site request forgery	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	352
11099	DOM-based cross-site scripting	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	79
11102	Cross-site request forgery	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	352
11114	DOM-based cross-site scripting	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	79
11119	DOM-based cross-site scripting	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	79
11120	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
11122	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
11098	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11105	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11108	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11118	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470
11126	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
11611	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
12468	Trust boundary violation	Low	01/24/20	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	501

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
11611	Unsafe deserialization	High	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	High impact security	Security	502
12468	Trust boundary violation	Low	01/24/20	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	501

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
12079	Unsafe reflection	Low	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Low impact security	Security	470

CID	Type	Impact	First Detected	Owner	Classification	Severity	Action	Component	Category	Issue Kind	CWE
10530	Open redirect	Medium	09/19/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Medium impact security	Security	601